INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-21 13:38 UTC

Ransomware Negotiators Acting as BlackCat/ALPHV Affiliates: Insider Threat in Incident Response Firms

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0193
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Organizations engaging third-party ransomware negotiation and incident response firms; confirmed victims include U.S. financial services firms, nonprofits, law firms, school districts, and medical facilities; firms implicated: DigitalMint and Sygnia
Published	2026-04-21T06:12:21
Discovery Source	Rss

Executive Summary

Three employees of ransomware negotiation firms DigitalMint and Sygnia pleaded guilty to operating simultaneously as BlackCat/ALPHV ransomware affiliates while serving as trusted incident response negotiators for victim organizations. These insiders fed confidential cyber insurance limits and live negotiation positions directly to ransomware operators, driving confirmed ransom payments of at least $25.6M from a financial services firm and $26.8M from a nonprofit. The core business risk is structural: any organization that invites a third-party negotiator into a live ransomware incident now faces an unverified insider channel with access to its most sensitive financial and operational deliberations.

Technical Analysis

No CVE or technical vulnerability is involved. The attack surface is organizational and procedural. Insiders holding legitimate IR engagement access (MITRE T1078, Valid Accounts) used their trusted position to exfiltrate negotiation-sensitive information, cyber insurance policy limits, ransom floor/ceiling positions, victim financial capacity, and relay that intelligence to BlackCat operators (T1591, Gather Victim Org Information; T1592, Gather Victim Host Information). This intelligence was used to anchor ransom demands above insurance coverage and prevent victims from negotiating effectively downward. The information exfiltration pathway was the trusted communication channel itself, not a technical exploit. Applicable CWEs reflect the process failures that enabled the scheme: CWE-284 (Improper Access Control, no separation between negotiator access and

sensitive financial disclosures), CWE-922 (Insecure Storage of Sensitive Information, insurance and negotiation data shared without compartmentalization controls), CWE-306 (Missing Authentication for Critical Function, no independent verification of negotiator firm personnel or conflict-of-interest screening), and CWE-693 (Protection Mechanism Failure, absence of third-party access monitoring during active engagements). The ransomware payload itself used T1486 (Data Encrypted for Impact) and T1489 (Service Stop). Data leak threats functioned as an additional extortion lever (T1567). The scheme operated over approximately a 2-year period from 2023 to 2025. DOJ prosecution is confirmed via guilty pleas. Primary source: DOJ Office of Public Affairs press release (T1 source).

Action Checklist

1. Step 1: Containment, If a third-party ransomware negotiator is currently engaged, immediately partition their access to cyber insurance policy documents, coverage limits, and live negotiation positions. Restrict that information to internal counsel and senior leadership only. Do not share ransom floor/ceiling thresholds with external parties unless legally required and independently verified.
2. Step 2: Detection, Review current and recent IR engagements for indicators of information leakage: ransom demands that precisely match or slightly exceed your disclosed insurance coverage limits; negotiation positions that appeared anchored against information only your internal team possessed; unusual escalation in ransom demands following negotiator briefings. Audit communication logs and document-sharing records for the active engagement period.
3. Step 3: Eradication, Terminate access for any third-party negotiation personnel who have not undergone formal conflict-of-interest screening and background verification. Require negotiation firms to provide written attestations confirming no affiliations with threat actor groups and no financial arrangements tied to ransom outcomes. Validate personnel credentials independently, do not rely solely on firm-level vetting.
4. Step 4: Recovery, After an engagement concludes, conduct a post-incident review of negotiation outcomes against internal financial disclosures to identify anomalies. Verify that ransom demands and settlement figures are consistent with what would be expected absent insider intelligence. Brief legal counsel on the DOJ case and assess whether prior engagements with DigitalMint or Sygnia warrant review.
5. Step 5: Post-Incident, Implement formal third-party IR vendor governance: conflict-of-interest declarations required before engagement, need-to-know compartmentalization for financial and insurance data, independent monitoring of negotiator communications during active incidents, and contractual liability clauses tied to information handling. Map these controls to NIST SP 800-53 PS-7 (Third-Party Personnel Security), AC-3 (Access Enforcement), and AU-12 (Audit Record Generation). Add negotiation firm personnel vetting to your ransomware response playbook as a prerequisite step before sharing any financial capacity information.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and FBI Cyber Division (tips.fbi.gov) immediately if: (1) a current ransomware engagement is active with DigitalMint or Sygnia personnel, (2) ransom demands in any past or current engagement are within 10% of disclosed cyber insurance limits suggesting insider anchoring, or (3) the organization qualifies as a covered entity under HIPAA, GLB, or state breach notification laws and ransom payments may have been inflated through insider leakage — constituting a potential civil fraud and regulatory disclosure obligation.
Recovery Notes	Post-containment, verify that no residual access exists for implicated negotiation firm personnel across all systems — including collaboration tools, email, VPN, and document repositories — and confirm via audit log review that no financial data was transmitted after access revocation was initiated. For organizations that engaged DigitalMint or Sygnia between 2018 and 2024 (the approximate window of the insider scheme per DOJ filings), retain all negotiation records and engage outside counsel to assess whether ransom overpayments constitute recoverable damages or insurance fraud claims. Monitor cryptocurrency wallet addresses used for prior ransom settlements against OFAC and FBI blockchain tracking advisories for 90 days post-incident, as ALPHV infrastructure reuse across victim payments has been documented by CISA.
Forensic Artifacts	Document sharing audit logs from Microsoft 365 Unified Audit Log (Search-UnifiedAuditLog -Operations FileAccessed,FileDownloaded,FilePreviewed) or Google Workspace Admin Reports — filtered to negotiation firm personnel UPNs and scoped to the engagement period — showing which insurance and financial documents were accessed, downloaded, or forwarded | Email transmission metadata (headers, recipient addresses, timestamps, attachment names) for all outbound messages from negotiation firm personnel to external addresses during the active incident, exported via Exchange Online PowerShell or Google Vault — specifically seeking transmissions to non-organizational domains coinciding with ransom demand escalations | Ransom demand timeline artifact: the original ransomware note (README.txt or equivalent ALPHV/BlackCat ransom note file, typically dropped in encrypted directories), plus all subsequent updated demands received through the negotiation channel, preserved with filesystem timestamps and hash values to establish the demand escalation sequence against the briefing timeline | Cryptocurrency transaction records for any ransom payments made — including the receiving wallet address, transaction ID, amount in BTC or Monero, and block confirmation timestamp — enabling cross-referencing against ALPHV-attributed wallet clusters identified in CISA Advisory AA23-353A (BlackCat/ALPHV) and FBI blockchain analysis | Negotiation firm engagement contract and fee schedule documentation — specifically any clauses referencing outcome-based compensation, percentage-of-savings arrangements, or success fees tied to ransom settlement amounts, which establish the financial motive underpinning the affiliate relationship documented in the DOJ guilty pleas

Per-Action IR Details

Step 1: Containment — If a third-party ransomware negotiator is currently engaged, immediately restrict their access to cyber insurance policy documents, coverage limits, and live negotiation positions. Compartmentalize that information to internal counsel and senior leadership only. Do not share ransom floor/ceiling thresholds with external parties unless legally required and independently verified.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate the channel through which insider-fed intelligence (cyber insurance limits, negotiation thresholds) flows to BlackCat/ALPHV operators by revoking external negotiator access to financial exposure data while the incident is active.

Controls: NIST AC-3 (Access Enforcement) — enforce least-privilege access so negotiation firm personnel (DigitalMint, Sygnia, or equivalents) cannot read cyber insurance policy documents or internal ransom floor/ceiling thresholds, NIST AC-6 (Least Privilege) — restrict insurance coverage limit visibility to internal legal counsel and senior leadership; no external party access absent documented legal necessity, NIST IR-4 (Incident Handling) — execute containment actions consistent with the incident response plan to prevent further leakage of financial capacity data to the threat actor, CIS 3.3 (Configure Data Access Control Lists) — apply access control lists to shared drives, SharePoint, or VDR folders containing cyber insurance schedules and negotiation briefs, removing external negotiator permissions immediately

Compensating: For teams without DLP or enterprise IAM: immediately revoke any shared drive links (Google Drive, SharePoint, Dropbox) distributed to negotiation firm personnel — do not merely change permissions, delete the share links entirely and audit link-sharing history. Run 'Get-SharingLinks' via SharePoint PowerShell or use the SharePoint admin portal to enumerate and revoke all externally shared items in the incident folder. For document repositories on Windows file servers, run 'Get-Acl | Format-List' for each sensitive directory and remove negotiator accounts. Store insurance policy documents offline (encrypted USB, air-gapped workstation) for the duration of the engagement.

Evidence: Before revoking access, preserve: (1) SharePoint/OneDrive audit logs showing which external accounts accessed insurance policy documents and negotiation briefs, including timestamps and file names — export via Microsoft Purview Audit (formerly Unified Audit Log) or 'Search-UnifiedAuditLog' PowerShell cmdlet filtering on Operations 'FileAccessed','FilePreviewed','FileDownloaded' for the negotiation firm personnel's UPN; (2) email thread metadata (not just body) showing what financial figures were transmitted to negotiator email domains (e.g., @digitalmint.io, @sygnia.co) — preserve as EML with headers; (3) VPN/remote access logs showing negotiator session timestamps correlated against ransom demand escalation events; (4) DocuSign or contract execution timestamps for negotiation engagement letters to establish when financial disclosures began.

Step 2: Detection — Review current and recent IR engagements for indicators of information leakage: ransom demands that precisely match or slightly exceed your disclosed insurance coverage limits; negotiation positions that appeared anchored against information only your internal team possessed; unusual escalation in ransom demands following negotiator briefings. Audit communication logs and document-sharing records for the active engagement period.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: analyze the behavioral pattern unique to this insider-affiliate scheme — ransom demand anchoring against disclosed insurance limits is the primary indicator of compromise distinguishing a corrupt negotiator from a standard ransomware negotiation.

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — systematically review document access logs, email send/receive records, and negotiation communication transcripts for the engagement period to identify correlation between negotiator briefings and demand escalations, NIST AU-2 (Event Logging) — verify that logging was enabled for file access on insurance documents and that email gateway logs captured outbound transmissions to negotiation firm domains during the incident window, NIST IR-5 (Incident Monitoring) — track and document each negotiation interaction as a discrete incident event, building a timeline that maps negotiator briefing moments against subsequent BlackCat/ALPHV demand changes, CIS 8.2 (Collect Audit Logs) — ensure audit logs from the email platform, document management system, and collaboration tools used during the engagement were retained and are available for the review period

Compensating: Without a SIEM: build a manual timeline in a spreadsheet with two parallel tracks — (1) internal briefing events: date/time negotiator was told insurance limit or negotiation position, sourced from email sent-items and meeting notes; (2) ransom demand history: date/time each demand was received from BlackCat/ALPHV operators. Compute the delta between briefing and demand change. A delta under 24 hours with demand anchoring to your disclosed limit is high-confidence evidence of leakage. For email analysis, use free tool 'MailExport' or Outlook's built-in export to PST, then parse with 'pffexport' (libpff) to extract headers. For Microsoft 365 without E5 licensing, run 'Search-UnifiedAuditLog -Operations Send -UserIds ' via Exchange Online PowerShell to identify outbound email from negotiator accounts.

Evidence: Preserve before analysis: (1) Full negotiation communication transcripts — all email threads, Signal/WhatsApp/Wire messages, and negotiation portal logs between your organization and BlackCat/ALPHV operators, timestamped to minute-level precision; (2) internal briefing records — calendar invites, meeting notes, or

Slack/Teams messages in which negotiator was informed of insurance limits or strategy positions, with exact figures disclosed; (3) ransomware operator demand history — each ransom note, updated demand, or counter-offer received from ALPHV infrastructure, preserved as original files with filesystem timestamps; (4) negotiation firm invoices or fee structures that could reveal success-fee or percentage-of-savings arrangements that create financial incentive aligned with higher ransom settlements.

Step 3: Eradication — Terminate access for any third-party negotiation personnel who have not undergone formal conflict-of-interest screening and background verification. Require negotiation firms to provide written attestations confirming no affiliations with threat actor groups and no financial arrangements tied to ransom outcomes. Validate personnel credentials independently — do not rely solely on firm-level vetting.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the insider threat vector by eliminating unvetted negotiator access to the environment; in this campaign the 'threat' is not malware but a trusted human with privileged access to financial intelligence, requiring personnel-level eradication actions rather than system remediation.

Controls: NIST PS-7 (External Personnel Security) — require negotiation firms to comply with organizational personnel security policies, including background screening and conflict-of-interest declarations, before personnel are granted access to sensitive incident data, NIST AC-2 (Account Management) — immediately disable or delete accounts, shared credentials, and collaboration platform memberships provisioned for negotiation firm personnel whose vetting status cannot be confirmed, NIST IR-4 (Incident Handling) — eradication actions must address the identified root cause; in this case the unvetted insider access channel is the threat component requiring removal, equivalent to removing malware persistence in a technical compromise, CIS 6.2 (Establish an Access Revoking Process) — execute the access revocation process for all negotiation firm personnel accounts across email, collaboration tools, VPN, and document repositories; do not leave dormant access in place pending attestation receipt, CIS 5.3 (Disable Dormant Accounts) — disable any negotiation firm accounts that remain active beyond engagement period or whose owners cannot be verified as currently engaged and vetted

Compensating: For teams without PAM or formal offboarding automation: create a checklist covering every access vector granted during the engagement — Microsoft 365 guest account, VPN credentials, shared Slack/Teams channel, Box/SharePoint folder permissions, Zoom external user access. Execute revocation sequentially and document each with a screenshot timestamp. For background verification without a commercial vendor: use PACER (pacer.gov, $0.10/page) to search federal criminal dockets for negotiation firm principals by name; cross-reference LinkedIn profiles against known BlackCat/ALPHV affiliate indictment names from the DOJ case (Hurley, Bhatt, Gubaidulin). Request a copy of the firm's SOC 2 Type II report and insurance certificate as a baseline trust indicator.

Evidence: Preserve before terminating access: (1) complete access provisioning records showing exactly what systems, documents, and data each negotiation firm employee was granted access to, and when — export from IAM system, Active Directory ('Get-ADUser -Properties MemberOf | Select MemberOf'), or Microsoft 365 admin portal; (2) screenshot or export of negotiation firm's engagement letter, scope of work, and any fee arrangements disclosed — specifically flag any language indicating outcome-based compensation tied to ransom settlement amounts; (3) any communications in which negotiation firm personnel requested information beyond what was operationally necessary for their stated role (e.g., asking for total cyber insurance schedule, not just the specific policy in play).

Step 4: Recovery — After an engagement concludes, conduct a post-incident review of negotiation outcomes against internal financial disclosures to identify anomalies. Verify that ransom demands and settlement figures are consistent with what would be expected absent insider intelligence. Brief legal counsel on the DOJ case and assess whether prior engagements with DigitalMint or Sygnia warrant review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: in this campaign recovery includes financial and legal integrity verification — organizations must confirm that ransom payments made were not inflated by insider intelligence leakage, and must assess exposure from prior engagements with implicated firms before returning to normal operations.

Controls: NIST IR-4 (Incident Handling) — recovery actions must include verification that the threat has been fully addressed; for this insider-affiliate scheme that means confirming no residual financial exposure or ongoing information

leakage to BlackCat/ALPHV infrastructure, NIST AU-11 (Audit Record Retention) — retain all negotiation-period logs, communications, and document access records for a minimum consistent with your incident retention policy and any potential DOJ civil or criminal proceedings related to the DigitalMint/Sygnia case, NIST CA-2 (Control Assessments) — assess whether existing third-party IR vendor controls were effective; identify which controls failed to detect the conflict of interest and document findings for remediation, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — treat the identified gap in third-party negotiator vetting as a process vulnerability requiring documented remediation with target completion date

Compensating: Without a forensic accounting capability: reconstruct the anomaly analysis manually by requesting from your cyber insurer the claims file showing what coverage limit was disclosed to the negotiation firm versus the final ransom settlement amount. If the settlement exceeds 80% of disclosed coverage limits, treat that ratio as an indicator warranting DOJ notification (contact FBI Cyber Division field office — tips.fbi.gov) rather than a coincidence. For prior DigitalMint or Sygnia engagements: pull past negotiation files and compare disclosed insurance limits (from the engagement kickoff documents) against final ransom payments; a consistent pattern of settlements near or above disclosed limits across multiple engagements is strong evidence of systematic leakage.

Evidence: Preserve for potential civil or criminal proceedings: (1) cyber insurance declarations page and coverage schedule as it existed at the time of the engagement — this establishes what financial limit was available for disclosure; (2) all ransom payment transaction records including cryptocurrency wallet addresses used for settlement, amounts in BTC/Monero, and blockchain transaction IDs — these can be cross-referenced against on-chain analytics tied to ALPHV infrastructure; (3) final ransom settlement amount versus initial ransom demand — the spread and anchoring relative to disclosed insurance limits is the core evidentiary fact pattern the DOJ used in the guilty pleas; (4) any cyber insurer communications acknowledging the coverage limit to the negotiation firm, which establishes the disclosure chain.

Step 5: Post-Incident — Implement formal third-party IR vendor governance: conflict-of-interest declarations required before engagement, need-to-know compartmentalization for financial and insurance data, independent monitoring of negotiator communications during active incidents, and contractual liability clauses tied to information handling. Map these controls to NIST SP 800-53 PS-7 (Third-Party Personnel Security), AC-3 (Access Enforcement), and AU-12 (Audit Record Generation). Add negotiation firm personnel vetting to your ransomware response playbook as a prerequisite step before sharing any financial capacity information.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned output must produce durable playbook changes that prevent recurrence; for this campaign the systemic failure was absence of conflict-of-interest controls over trusted third parties with privileged access to financial intelligence during high-stakes incidents.

Controls: NIST PS-7 (External Personnel Security) — require conflict-of-interest declarations, background checks, and contractual security obligations from negotiation firm personnel before granting any access to insurance or financial data, NIST AC-3 (Access Enforcement) — enforce logical access controls ensuring negotiation firm personnel can only access information explicitly required for their negotiation role, with insurance policy documents restricted to internal counsel, NIST AU-12 (Audit Record Generation) — configure audit record generation for all systems accessed by third-party negotiation personnel during active engagements, capturing file access, download, and transmission events, NIST IR-8 (Incident Response Plan) — update the ransomware response playbook to include negotiation firm vetting as a formal prerequisite gate before any financial capacity information is shared with external parties, NIST SA-9 (External System Services) — establish contractual requirements for negotiation firms that include information handling obligations, conflict-of-interest prohibitions, and audit rights consistent with the risks demonstrated in the DigitalMint/Sygnia case, CIS 6.1 (Establish an Access Granting Process) — add negotiation firm personnel to the formal access granting workflow with a conflict-of-interest clearance step as a mandatory gate before provisioning, CIS 3.3 (Configure Data Access Control Lists) — enforce ACLs on all repositories containing insurance schedules, coverage limits, and negotiation strategy documents to prevent unauthorized access by external parties

Compensating: For teams without a GRC platform to manage third-party risk: create a one-page 'Ransomware Negotiator Onboarding Checklist' in your incident response binder with mandatory fields: (1) firm name and individual negotiator names; (2) PACER/criminal background check confirmation; (3) signed conflict-of-interest declaration (template available from ACFE — acfe.com); (4) fee structure review confirming no outcome-based compensation tied

to ransom amount; (5) list of specific documents authorized for sharing, with insurance policy documents explicitly excluded absent legal sign-off. Store signed declarations in a dedicated evidence-quality folder (write-once if possible) accessible only to legal and IR leadership. For communications monitoring without an enterprise DLP solution: require all negotiator communications with the threat actor to be conducted via a dedicated, organization-controlled email account (not the negotiator's personal firm account) so full thread visibility is maintained internally.

Evidence: For the post-incident record and future audit readiness: (1) document the specific financial disclosures made to negotiation firm personnel during the incident, cross-referenced against subsequent ransom demand changes — this becomes the evidentiary baseline for assessing whether the new controls would have detected leakage; (2) retain all engagement contracts with DigitalMint or Sygnia personnel who have pleaded guilty — DOJ case reference: U.S. v. Hurley et al. — as documentation of the known-bad third-party relationship for regulatory disclosure purposes; (3) preserve the lessons-learned report itself with date and executive sign-off as evidence of NIST IR-4 (Incident Handling) compliance for any future regulatory inquiry or cyber insurance renewal.

Detection Guidance

No technical IOCs are available for this campaign. Detection is behavioral and procedural. Indicators of compromise in this context are informational, not technical: (1) Ransom demands that match or marginally exceed your organization's cyber insurance coverage limit, this is a primary signal that insurance data was disclosed to threat actors. (2) Negotiation positions that appear to track your internal floor/ceiling thresholds in real time. (3) Threat actor communications that reference specific financial details your organization shared only with the negotiation firm. For ongoing engagements, implement a deliberate information compartmentalization test: provide the negotiation firm a slightly incorrect insurance figure and monitor whether subsequent ransom demands reflect that figure. Log all document sharing with external IR parties during active incidents. For past engagements involving DigitalMint or Sygnia personnel named in the DOJ indictment, review ransom settlement amounts against internal financial disclosures and consult legal counsel.

Framework Mappings

MITRE-ATTACK

- **T1592** — Gather Victim Host Information
- **T1489** — Service Stop
- **T1078** — Valid Accounts
- **T1657** — Financial Theft
- **T1583** — Acquire Infrastructure
- **T1591** — Gather Victim Org Information
- **T1567** — Exfiltration Over Web Service
- **T1199** — Trusted Relationship
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **SC-7** — Boundary Protection
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **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
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1592	Gather Victim Host Information	Reconnaissance
T1489	Service Stop	Impact
T1078	Valid Accounts	Defense-Evasion
T1657	Financial Theft	Impact
T1583	Acquire Infrastructure	Resource-Development
T1591	Gather Victim Org Information	Reconnaissance
T1567	Exfiltration Over Web Service	Exfiltration
T1199	Trusted Relationship	Initial-Access
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/former-ransomware-ne...	T3
Two Americans Plead Guilty to Targeting Multiple U.S. Victims Using ...	https://www.justice.gov/opa/pr/two-americans-plead-guilty-targeting...	T1
Third Ransomware Negotiator Charged Over Involvement with ...	https://www.hipaajournal.com/u-s-nationals-indicted-blackcat-ransom...	T3
DigitalMint and Sygnia Cybersecurity Insiders Indicted for ALPHV ...	https://www.rescana.com/post/digitalmint-and-sygnia-cybersecurity-i...	T3
US cybersecurity experts indicted for BlackCat ransomware attacks	https://www.bleepingcomputer.com/news/security/us-cybersecurity-exp...	T3

Generated 2026-04-21 13:38 UTC by TJS Security Command Center