



● CONFIDENTIAL — AUTHORISED RECIPIENTS ONLY

FRAUD INVESTIGATION

Ransomware Victim Recovery Briefing — STOP/DJVV Variant, Columbus OH

Subject: Unknown ransomware operator · Jurisdiction: Columbus, Ohio, USA

EXECUTIVE SUMMARY

This is a STOP/DJVV ransomware incident affecting a student in Columbus, Ohio — a low-complexity US jurisdiction with excellent free resources available. The operative challenge is not investigative but technical: whether the encrypted files can be recovered without payment.

TARGET LOCATION

Columbus, Ohio, USA

CLIENT TYPE

other

URGENCY

urgent, same day

BUDGET

Free

REFERENCE

OPS-CKT5PZ

ENRICHMENT

1 of 9 sources returned data

JURISDICTION ASSESSMENT

COMPLEXITY

LOW

SERVICES

EXCELLENT

THREAT LEVEL

MEDIUM

SOURCES QUERIED

SEC EDGAR (Securities Filings)	GLEIF (Legal Entity Identifier)	Wikidata (Structured Entity Data)
Wikipedia (Identity Resolution)	Companies House (UK Corporate Registry)	UK Insolvency & Disqualification
Courtlistener (US Federal Courts)	SAM.gov (Federal Debarments)	HaveIBeenPwned (Email Breaches)





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

Ransomware Victim Recovery Briefing — STOP/DJVU Variant, Columbus OH

COMPLEXITY RATING

LOW

SERVICES AVAILABILITY

EXCELLENT

THREAT LEVEL

MEDIUM

KEY FINDINGS & NEXT STEPS

KEY FINDINGS

- The decryptability of the files depends on one critical technical variable: whether the ransomware used an "offline key" or an "online key" during encryption.
- Offline keys are universal across victims and have been largely recovered by Emsisoft.
- Online keys are unique per victim and cannot currently be decrypted for free.
- The university IT department is the most underutilised free resource in this scenario.

NEXT STEPS

- Visit nomoreransom.org today and run the Crypto Sheriff tool using two encrypted files and the `_readme.txt` to confirm the variant and available decryptors.
- Contact the university IT helpdesk today, identify this as a ransomware incident with a dissertation deadline, and ask specifically about institutional cloud backups and student endpoint recovery tools.
- File a complaint at ic3.gov and report to reportfraud.ftc.gov to create an official record at no cost.

MATTER SUMMARY

A final-year university student in Columbus, Ohio has had their primary working device encrypted by ransomware following installation of cracked software. The ransom demand — \$980, or \$490 within 72 hours — follows the precise pricing structure of the STOP/DJVU ransomware family, one of the most prolific consumer-targeting strains globally. The contact email addresses provided (restorehelp.manager@mx-recover9.top and datarestore.support@relaybox7.cc) are consistent with STOP/DJVU operator infrastructure. With a dissertation deadline in three weeks and approximately \$61 available, the client cannot pay the ransom, cannot afford professional recovery services, and is operating under acute time pressure.

The core challenge is not investigative — the ransomware operator is effectively anonymous and beyond civil reach — but technical and practical: whether decryption is possible without payment, and how to protect and recover what data can be salvaged. Four years of academic work, including a near-complete dissertation, are at risk. This briefing is structured accordingly: the investigative framing is acknowledged but the operative priority is immediate, zero-cost data recovery using every free resource currently available to the client.

JURISDICTION PROFILE

Country: United States of America

City: Columbus, Ohio

Complexity Rating: LOW

Professional Services Availability: EXCELLENT

Threat Level: MEDIUM (to data; LOW to personal safety)





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

THRESHOLD ASSESSMENT

WHAT MUST HAPPEN IN THE TARGET JURISDICTION:

Nothing. There is no civil or criminal action the client can meaningfully pursue against an anonymous ransomware operator that requires local legal presence. Even if the operator were identified, enforcement against cybercriminal actors typically proceeds through federal channels (FBI/IC3), not local civil litigation. Filing a police report in Columbus is a one-step self-directed action requiring no professional. No task in this matter genuinely requires hiring a local professional.

WHAT CAN BE DONE REMOTELY OR FROM THE CLIENT'S OWN JURISDICTION:

Everything substantive. Decryption tool searches, submission to the No More Ransom project, identification checking against STOP/DJVU decryptor databases, and reporting to IC3 are all entirely remote and self-directed. The client is already in the relevant jurisdiction and can take every meaningful action from their own device or phone.

WHAT THE CLIENT CAN DO THEMSELVES, TODAY, AT NO COST:

- Identify the exact STOP/DJVU variant from the file extension and the _readme.txt, then check the No More Ransom decryption tool database immediately.
- Submit an encrypted file sample and the _readme.txt to Emsisoft's free STOP/DJVU decryptor tool, which has successfully recovered files for hundreds of thousands of victims.
- Check whether any files were backed up to OneDrive, Google Drive, email attachments, or a USB drive at any prior point — even partial recovery changes the situation.
- Report to the FBI Internet Crime Complaint Center (IC3) at ic3.gov — this costs nothing and creates an official record.
- Report to the FTC at reportfraud.ftc.gov — also free and creates a reference number for any future insurance or institutional claim.
- Contact their university's IT department immediately — many universities have enterprise backup tools or shadow copy access that students are unaware of, and the university may have a cybersecurity incident team.
- Check Windows Volume Shadow Copies using free tools (ShadowExplorer) before any further writes to the disk, as some STOP/DJVU variants do not successfully delete all shadow copies.
- Do NOT pay the ransom. Payment does not guarantee decryption, funds criminal infrastructure, and in some variants the decryption key is never delivered.

PROPORTIONALITY:

The financial value at stake is not the \$980 ransom or the \$1,200 repair quote — both exceed the client's resources. The true value at stake is four years of irreplaceable academic work and a dissertation with a three-week deadline. That is high personal stakes but not a recoverable financial sum that would justify professional engagement. The matter is explicitly disproportionate to professional investigation fees. The only proportionate track is self-directed, free-tool recovery.

THRESHOLD CONCLUSION:

This matter does not require engagement in the target jurisdiction in any professional capacity. It is a self-directed technical recovery matter. The client's immediate priority is to attempt decryption using the Emsisoft STOP/DJVU tool and No More Ransom resources before the deadline. Reporting to IC3 and the university IT department are secondary but same-day actions. No paid professional is required or recommended as a primary approach.

KEY CONSIDERATIONS

1. STOP/DJVU identification is near-certain based on the evidence. The \$980/\$490 pricing, the 72-hour window, the _readme.txt filename, and the dual-email contact pattern are hallmarks of STOP/DJVU. This matters because a dedicated free decryptor exists for many variants of this family — identification determines whether decryption is possible at all.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

2. The decryptability of the files depends on one critical technical variable: whether the ransomware used an "offline key" or an "online key" during encryption. Offline keys are universal across victims and have been largely recovered by Emsisoft. Online keys are unique per victim and cannot currently be decrypted for free. The client must run the Emsisoft tool to determine which applies.

3. The contact email domains (mx-recover9.top and relaybox7.cc) were checked against the Have I Been Pwned breach database. No breach records were found for either address. This result is neutral — it does not indicate the operators are trustworthy or that payment would result in decryption. It means only that these specific addresses have not appeared in known data breach datasets. The check confirms the identifiers were processed; it returns no adverse or positive intelligence about the operators themselves.

4. Live database screening returned no adverse findings of investigative significance. No federal court records were identified via CourtListener. No federal debarment or exclusion was found via SAM.gov — confirmed via the official US federal registry. No legal entity identifier was found via GLEIF, which is entirely expected for a criminal actor operating anonymously. Interpol Red Notice and ICIJ checks were unavailable, so no conclusion can be drawn from those sources. Collectively, the database environment provides no investigative lead that would assist identification or civil recovery.

5. The university IT department is the most underutilised free resource in this scenario. Many institutions run automated cloud backups of student files, operate licensed antivirus and endpoint recovery tools, and have cybersecurity staff trained for exactly this situation. This contact should happen today, before any further action is taken on the device.

STRATEGIC APPROACHES

APPROACH 1 — STANDARD

Method: Self-directed free tool recovery. Run Emsisoft STOP/DJVU Decryptor, check No More Ransom portal, run ShadowExplorer for VSS recovery, recover from any cloud/email backup, report to IC3 and university IT.

Timeline: Same day to 72 hours.

Estimated Cost: \$0.

Recommended for: This client. This is the only proportionate approach given the budget and the nature of the threat.

APPROACH 2 — ACCELERATED (RECOMMENDED)

Method: Same as Approach 1, plus direct engagement with university IT security team for institutional backup access and campus cybersecurity clinic if available. Some universities partner with Emsisoft or similar vendors under enterprise agreements. Also submit to BleepingComputer STOP/DJVU forum thread for community expert triage.

Timeline: 24–48 hours.

Estimated Cost: \$0.

Recommended for: All clients at this budget tier. The university engagement costs nothing and may unlock institutional tools unavailable to the public.

APPROACH 3 — EXPEDITED

Method: If Approaches 1 and 2 fail and files remain encrypted, contact local nonprofit tech clinics (e.g., university makerspace, IEEE student chapter, CompTIA-certified volunteer programs) for supervised recovery attempt. As a last resort before the deadline, prioritise reconstructing the dissertation from any recoverable fragments, draft notes, email attachments, printed copies, or supervisor correspondence.

Timeline: Days 3–10.

Estimated Cost: \$0 (volunteer/nonprofit).

Recommended for: Scenario where decryption is not possible and deadline survival requires content reconstruction rather than technical recovery.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

LEGAL & REGULATORY FRAMEWORK

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, criminalises the deployment of ransomware at the federal level. The FBI's Cyber Division and the Internet Crime Complaint Center (IC3) are the primary federal reporting bodies. Columbus, Ohio falls under the Southern District of Ohio for federal matters and the Ohio Attorney General's cybercrime unit at the state level. Reporting to IC3 does not guarantee an investigation of this specific matter — ransomware complaints are aggregated to build threat intelligence and occasionally support larger enforcement actions — but filing costs nothing and is the correct procedural step.

Ohio does not impose a legal obligation on individuals to report ransomware infections, but reporting to both IC3 and the FTC creates a record that may assist in any future insurance claim, academic accommodation request, or university incident process. The ransom demand itself constitutes extortion under federal law. Paying the ransom is not illegal for a private individual, but it carries no guarantee of file recovery and is strongly discouraged by the FBI, CISA, and all major cybersecurity agencies.

No civil action against the operator is realistically available to this client. Even if the operator were identified — which is unlikely given the anonymous infrastructure of STOP/DJVVU campaigns — civil litigation would require funds the client does not have, would take years, and collection against a criminal actor is nearly impossible. The legal framework here is relevant primarily as a reporting pathway, not a recovery mechanism.

PROFESSIONAL SERVICE PROVIDERS REQUIRED

TYPE: None required as a primary engagement.

ROLE: All immediate recovery actions are self-directed.

QUALIFICATIONS TO LOOK FOR: N/A

TYPICAL COST RANGE: \$0

HOW TO VERIFY CREDENTIALS: N/A

CONFIDENCE LEVEL: HIGH

TYPE: University IT Security / Helpdesk (internal, not a paid provider)

ROLE: Access institutional backup systems, run licensed recovery tools, advise on campus cybersecurity resources.

QUALIFICATIONS TO LOOK FOR: University-employed IT staff — no credential verification required by the client.

TYPICAL COST RANGE: \$0 (included in university services)

HOW TO VERIFY CREDENTIALS: Contact via official university IT portal or student services helpdesk.

CONFIDENCE LEVEL: HIGH

RECOMMENDED LOCAL FIRMS & CONTACTS

SERVICE TYPE: Federal Reporting Portal

FIRM NAME: FBI Internet Crime Complaint Center

WEBSITE: ic3.gov

WHY SUITABLE: The correct federal reporting channel for ransomware in the United States. Free, anonymous, and generates a complaint reference number.

HOW TO MAKE CONTACT: Online complaint form at ic3.gov.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: Free Ransomware Decryption Resource

FIRM NAME: No More Ransom Project

WEBSITE: nomoreransom.org

WHY SUITABLE: EU-law-enforcement-backed portal aggregating free decryptors for hundreds of ransomware families including STOP/DJVVU. First port of call for any ransomware victim globally.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

HOW TO MAKE CONTACT: Upload encrypted file sample directly via the website's Crypto Sheriff tool.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: Free STOP/DJVVU Decryptor

FIRM NAME: Emsisoft

WEBSITE: emsisoft.com

WHY SUITABLE: Emsisoft developed and maintains the primary free decryptor for STOP/DJVVU variants. Has recovered files for over a million victims. Offline-key variants are fully recoverable; online-key variants require waiting for future key releases.

HOW TO MAKE CONTACT: Download decryptor directly from emsisoft.com; community support available via BleepingComputer forum thread specifically for STOP/DJVVU.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: Consumer Fraud Reporting

FIRM NAME: Federal Trade Commission ReportFraud Portal

WEBSITE: reportfraud.ftc.gov

WHY SUITABLE: US federal consumer protection reporting — free, generates a reference number, and contributes to enforcement data.

HOW TO MAKE CONTACT: Online form at reportfraud.ftc.gov.

CONFIDENCE LEVEL: HIGH

SERVICE TYPE: Community Technical Support

FIRM NAME: BleepingComputer Forums

WEBSITE: bleepingcomputer.com

WHY SUITABLE: The leading free community resource for ransomware victims. Dedicated STOP/DJVVU support thread with expert volunteers who can confirm variant, advise on decryptability, and guide recovery steps.

HOW TO MAKE CONTACT: Register and post in the ransomware help subforum; reference the file extension and paste the _readme.txt content.

CONFIDENCE LEVEL: HIGH

RISK & COMPLIANCE CONSIDERATIONS

The live intelligence environment for this matter is sparse in a way that is both expected and operationally significant. No adverse findings were returned in any database that was successfully queried. No federal court records were identified via CourtListener. No federal debarment or exclusion was found via SAM.gov. No legal entity identifier was found via GLEIF — which is entirely normal for a criminal operator who is not a registered entity. These are null results in the investigative sense: they do not indicate low risk from the operator, they indicate the operator has no formal institutional footprint that could be traced through conventional registry channels. The Interpol Red Notice check was unavailable, and no conclusion can be drawn from that source.

The email addresses used as contact identifiers — restorehelp.manager@mx-recover9.top and datastore.support@relaybox7.cc — were checked against the Have I Been Pwned breach database. No breach records were found for either address. This is a clean result from that specific check, not an assessment of the operators' credibility or reliability. It should be read narrowly: these addresses have not appeared in known breach datasets, nothing more. The domains (mx-recover9.top and relaybox7.cc) are consistent with the disposable, rotating infrastructure typical of STOP/DJVVU campaigns and should be treated as untrustworthy regardless of the HIBP result.

The client should be alert to secondary scam risk. Ransomware victims are frequently targeted by fraudulent "recovery services" that charge significant upfront fees and deliver nothing. Any service charging money upfront to recover STOP/DJVVU files should be treated with extreme suspicion — legitimate tools from Emsisoft and No More Ransom are free. The \$1,200 quote from the local repair shop may represent a legitimate service, but the same outcome may be achievable at no cost through the tools identified in this briefing.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

LOCAL CONTEXT

Columbus, Ohio is home to Ohio State University and a substantial technology and cybersecurity professional community. The city has active chapters of cybersecurity professional organisations and student-run technology assistance programmes. University IT departments in Ohio's major academic institutions are generally well-resourced and familiar with ransomware incidents among the student population — STOP/DJVV in particular is endemic among students who install cracked software, and IT staff at institutions like OSU will have encountered this exact situation repeatedly.

The broader Columbus environment is favourable for self-directed recovery. BleepingComputer and the No More Ransom project are accessible without geographic restriction. Ohio's Attorney General operates a cybercrime reporting unit, and CISA (the federal Cybersecurity and Infrastructure Security Agency) offers free resources including direct advisory support for individuals affected by ransomware. None of these require the client to spend money.

SECURE WORKING PRACTICES

Do not connect the infected device to any network, shared drive, or university system until it has been assessed — STOP/DJVV does not typically spread laterally, but the device may have additional malware from the same cracked software installation. Run all recovery tools from a clean USB drive if possible, or download them to a separate device. Do not communicate with the ransomware operators via the provided email addresses — doing so confirms the address is active and may invite further social engineering. Do not pay any third-party "recovery service" that contacts the client proactively, as this is a known secondary scam pattern targeting ransomware victims.

RECOMMENDED APPROACH

The recommended approach is entirely self-directed and costs nothing. Execute the following steps in order, same day:

1. Note the exact file extension added to encrypted files — this is the variant identifier.
2. Visit nomoreransom.org and use the Crypto Sheriff tool to upload two encrypted files and the _readme.txt. The portal will confirm whether a free decryptor exists.
3. Download the Emsisoft STOP/DJVV Decryptor from emsisoft.com and run it — this is the definitive free tool for this family and handles variant identification automatically.
4. Run ShadowExplorer (shadowexplorer.com, free) to check whether Windows Volume Shadow Copies survived — some STOP/DJVV variants fail to delete all shadow copies.
5. Check every cloud storage account (OneDrive, Google Drive, Dropbox), email sent folder, and any USB drive ever used with the device for any version of dissertation files.
6. Contact the university IT helpdesk today — explain it is a ransomware incident with a dissertation deadline, and ask specifically about institutional cloud backups and student endpoint protection tools.

If decryption is confirmed as impossible (online key variant, no shadow copies, no cloud backup), shift immediately to content reconstruction. Contact the dissertation supervisor to confirm whether any draft chapters were submitted by email. Check the university's virtual learning environment (Canvas, Blackboard, Moodle) for any submitted drafts. Retrieve any printed copies. Three weeks is a workable reconstruction window if partial content can be recovered.

Report the incident to IC3 at [ic3.gov](https://www.ic3.gov) and to the FTC at [reportfraud.ftc.gov](https://www.reportfraud.ftc.gov). These reports cost nothing, take under 30 minutes, and create an official record that may support any university accommodation request or future insurance claim. Keep all reference numbers.





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

TIMELINE & MILESTONES

- (1) Day 1 (today): Run No More Ransom Crypto Sheriff and Emsisoft STOP/DJVVU Decryptor. Run ShadowExplorer. Contact university IT helpdesk. Check all cloud storage.
- (2) Days 1–2: Receive IT department response. Determine decryptability (offline key = recovery likely; online key = pivot to reconstruction).
- (3) Days 2–3: If decryption succeeds, back up all recovered files immediately to at least two separate locations. File IC3 and FTC reports.
- (4) Days 3–7: If decryption fails, begin dissertation reconstruction using supervisor emails, VLE submissions, printed drafts, and notes. Contact dissertation supervisor to explain the situation and request accommodation if needed.
- (5) Days 7–21: Complete dissertation reconstruction or final editing of recovered content ahead of deadline. Maintain clean backup discipline from this point forward.

Confidence rating: HIGH that free tools will resolve the question of decryptability within 24 hours. Outcome confidence is MEDIUM — dependent on whether the variant used an offline or online encryption key, which cannot be determined without running the tool.

CONTINGENCY CONSIDERATIONS

If the Emsisoft tool confirms an online key variant and no backup exists, decryption is not currently possible for free. The client should check the Emsisoft STOP/DJVVU forum thread at BleepingComputer periodically — Emsisoft releases new keys as law enforcement operations recover them, and victims have had files decrypted months after initial infection. Submitting the encrypted file and ID to Emsisoft's victim database ensures the client will benefit from any future key release. The dissertation deadline, however, requires a parallel reconstruction track to begin immediately rather than waiting for a future key release.

If professional investigative support ever becomes necessary — for example if this matter escalates or the client's institution pursues a formal complaint — vetted local cybersecurity professionals and digital forensics investigators can be located through the ACFE CFE Finder at [acfe.com](https://www.acfe.com), the High Technology Crime Investigation Association member directory at htcia.org, or the (ISC)² member directory at isc2.org. These directories allow searches by location and specialty and carry credential verification. No paid engagement is recommended or necessary for this matter as it currently stands.

PROFESSIONAL FEES ESTIMATE

This matter requires no professional expenditure. Every action identified as proportionate and effective in this briefing is free. The Emsisoft decryptor, No More Ransom portal, ShadowExplorer, IC3 reporting, FTC reporting, and university IT engagement all carry zero cost. The client's \$61 should not be spent on this matter — there is no paid service at that price point that would outperform the free tools available.

If decryption fails and the client later wishes to pursue data forensics professionally, entry-level data recovery services in Columbus start at approximately \$300–\$500 for a desktop assessment, rising significantly for encrypted drive recovery. This would exceed the client's current budget and is not recommended unless the client can secure additional funds — for example through a university emergency hardship fund, of which many Ohio institutions have one specifically for technology emergencies.

EXECUTIVE SUMMARY & RECOMMENDED NEXT STEPS

This is a STOP/DJVVU ransomware incident affecting a student in Columbus, Ohio — a low-complexity US jurisdiction with excellent free resources available. The operative challenge is not investigative but technical: whether the encrypted files can be recovered without payment. Live database screening returned no adverse findings of investigative value against the operator, and the contact emails produced no breach records in the Have I Been Pwned check — results that are neutral and expected for an anonymous criminal





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

infrastructure, not indicators of operator trustworthiness. The Interpol Red Notice check was unavailable, so no conclusion can be drawn from that source, and no sanctions screening was performed by this system. The recommended approach is entirely self-directed and costs nothing: the Emsisoft STOP/DJVM Decryptor and the No More Ransom project are the decisive first steps, followed immediately by university IT engagement and shadow copy recovery attempts.

1. Visit nomoreransom.org today and run the Crypto Sheriff tool using two encrypted files and the `_readme.txt` to confirm the variant and available decryptors.
2. Download and run the Emsisoft STOP/DJVM Decryptor from emsisoft.com to determine whether an offline or online key was used and, where possible, to decrypt files immediately.
3. Contact the university IT helpdesk today, identify this as a ransomware incident with a dissertation deadline, and ask specifically about institutional cloud backups and student endpoint recovery tools.
4. File a complaint at ic3.gov and report to reportfraud.ftc.gov to create an official record at no cost.
5. If decryption is not immediately possible, begin dissertation reconstruction in parallel using supervisor emails, VLE submissions, and any printed drafts, and request a formal accommodation from the dissertation supervisor.

If the recommended approach is followed, the client has a realistic prospect of recovering their files at no cost within 24–72 hours if the variant used an offline encryption key — and a clear fallback reconstruction path if it did not.

--- END OF BRIEFING ---

[*] LIVE INTELLIGENCE ENRICHMENT

Live data from public sources, jurisdiction-routed, verify independently before operational use

> [!] IMPORTANT – READ BEFORE USING THIS DATA
> All results below are name-matched only. They are retrieved by querying public databases with the subject name as a search string. They have NOT been verified as relating to the specific individual or entity named in this engagement. Results may refer to entirely different people or companies who share the same name.
>
> Before relying on any finding below: cross-reference against date of birth, company registration number, address, or other known identifiers to confirm the result relates to your subject. Use the manual registry links provided in each section to verify directly at source.
>
> On absence of results: a source returning no match means only that this specific database holds no record matching the search string. It is not evidence of absence of risk. Small and mid-size private entities are routinely absent from LEI, encyclopaedia and news sources – this is expected and carries no adverse inference. Sections marked [!] require identity verification before operational use.
Live data retrieved from public sources. All findings require independent verification before operational use.

INTELLIGENCE SOURCE MANIFEST

Complete record of every source queried for this report – what triggered it and its current status.

SOURCE	TRIGGER	STATUS
---	---	---



CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

Interpol Red Notices	Always active	[!] Source could not be reached
ICIJ Offshore Leaks	Always active	[!] Source could not be reached
GLEIF (Legal Entity Identifier)	Always active	[OK] No matches
Google News RSS	Always active	[!] Source could not be reached
Wikidata (Structured Entity Data)	Always active	[OK] No records found
Wikipedia (Identity Resolution)	Always active – title prefilter and resolver review	
[OK] No candidates returned by opensearch		
Companies House (UK Corporate Registry)	UK location OR British nationality	Not
queried – no UK connection detected		
UK Insolvency & Disqualification	UK location OR British nationality	Not queried –
no UK connection detected		
CourtListener (US Federal Courts)	US location OR American nationality	[OK] No matches
SEC EDGAR (Securities Filings)	US location OR American nationality	8 candidates - 0
matched, 0 unresolved, 8 excluded		
SAM.gov (Federal Debarments)	US location OR American nationality	[OK] No debarments
HaveIBeenPwned (Email Breaches)	Email field provided	[OK] No breaches found
IP Geolocation (Domain Server)	Domain field provided	– Not activated (provide domain
to enable)		
EU VIES VAT Registry	EU VAT number field provided	– Not activated (provide VAT number
to enable) |
Direct integration for OpenSanctions, OpenCorporates and additional registries is in
development. Until then, use the pre-targeted verification links in each section above.

JURISDICTION ROUTING NOTE

Jurisdiction-specific sources NOT queried (not applicable to this subject):

- Companies House (UK-registered companies only)
- UK Insolvency Service (UK subjects only)

ENTITY PROFILE

Wikidata indexes notable public entities only; absence is expected for private companies and individuals.

WIKIPEDIA PROFILE

Wikipedia returned no candidate articles for this search. Absence from Wikipedia is expected for private companies and non-public individuals and carries no adverse inference.

INTERPOL RED NOTICES

The Interpol source could not be reached. No conclusion is drawn from this unavailable query.

GLOBAL COMPANY REGISTRY

Global registry search is not automated in this report. UK registrations are covered by the Companies House section where applicable. For other jurisdictions, search directly:

- OpenCorporates: <https://opencorporates.com/companies?q=Unknown%20ransomware%20operator>

LEGAL ENTITY IDENTIFIER

GLEIF has returned no Legal Entity Identifier records matching "Unknown ransomware operator". Subject may not be a LEI-registered entity, or may be registered under a variant





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

name.

SANCTIONS / PEP SCREENING

Automated sanctions screening is not performed by this report. Screen the subject directly against the consolidated lists below before any commercial or operational commitment:

- OpenSanctions (aggregated global):

<https://www.opensanctions.org/search/?q=Unknown%20ransomware%20operator>

- UK OFSI Consolidated List:

<https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets>

- US OFAC SDN Search: <https://sanctionssearch.ofac.treas.gov/>

- EU Consolidated Sanctions List: <https://www.sanctionsmap.eu/>

OFFSHORE LEAKS DATABASE

The ICIJ Offshore Leaks source could not be reached. No conclusion is drawn from this unavailable query.

RECENT NEWS INTELLIGENCE

The Google News source could not be reached. No absence-of-news conclusion is drawn from this unavailable query.

EXCLUDED IDENTITY COLLISION ARTIFACTS

The following retrieved records remain visible for auditability but are excluded from analysis of the client subject:

- 8 court or securities records withheld as name-collision artifacts; captions and filer details are not reproduced.

DIRECTORSHIP HISTORY

Global officer search is not automated in this report. UK officer appointments appear in the Companies House section where applicable. For other jurisdictions:

- OpenCorporates Officers:

<https://opencorporates.com/officers?q=Unknown%20ransomware%20operator>

SEC / EDGAR FILINGS

0 of 8 filings returned were filed by the client subject. 8 records were mentions or name-collision results and are not reproduced.

Full EDGAR search:

<https://efits.sec.gov/LATEST/search-index?q=%22Unknown%20ransomware%20operator%22>

FEDERAL DEBARMENT / EXCLUSIONS

SAM.gov has returned no matches for "Unknown ransomware operator" on the US Federal Excluded Parties List.

Manual search:

https://sam.gov/search/?keywords=Unknown%20ransomware%20operator&sort=relevance&index=ex&is_active=true&page=1

COURT RECORD HITS

CourtListener has returned no matching records in US federal court dockets for "Unknown ransomware operator".





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

EMAIL BREACH SCREENING

HaveIBeenPwned has returned no breach records for `restorehelp.manager@mx-recover9.top`, `datastore.support@relaybox7.cc`. Email address does not appear in any known data breach at time of query.

SUBJECT LOCATION INTELLIGENCE

The following represents documented and inferred location signals for subject: Unknown ransomware operator

DOCUMENTED LOCATION SIGNALS:

- (1) Reported last known area: Columbus, Ohio, USA
- (2) Jurisdiction routing signal supplied: american

NOTE: Location signals are derived from public records and may be outdated. A registered address confirms a filing position, not a physical trading presence. Confirm independently before relying on any location above.

INVESTIGATOR REGISTRY LINKS

Pre-constructed links for manual investigator follow-up. Jurisdiction-aware – only relevant registries shown for this location, nationality, and operation type.

Global Registries

- (1) OpenCorporates – Global Company Search:

<https://opencorporates.com/companies?q=Unknown%20ransomware%20operator>

- (2) OpenSanctions – Sanctions & PEP Database:

<https://www.opensanctions.org/search/?q=Unknown%20ransomware%20operator>

- (3) ICIJ Offshore Leaks – Panama/Pandora Papers:

<https://offshoreleaks.icij.org/search?q=Unknown%20ransomware%20operator>

- (4) OCCRP Aleph – Investigative Journalism Database:

<https://aleph.occrp.org/search?q=Unknown%20ransomware%20operator>

- (5) GLEIF – Legal Entity Identifier Database:

<https://search.gleif.org/#/record/search?query=Unknown%20ransomware%20operator>

- (6) Interpol Red Notices: <https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices>

- (7) World-Check (Thomson Reuters):

<https://www.refinitiv.com/en/financial-risk/screening-solutions/world-check-kyc-screening>

US Federal & State Registries

- (1) PACER – Federal Court Dockets: <https://pacer.uscourts.gov/>

- (2) CourtListener – Free Federal Records:

https://www.courtlistener.com/?q=Unknown%20ransomware%20operator&type=r&order_by=score+desc

- (3) EDGAR (SEC) – Securities Filings:

<https://efits.sec.gov/LATEST/search-index?q=%22Unknown%20ransomware%20operator%22>

- (4) SAM.gov – Federal Debarments & Exclusions:

https://sam.gov/search/?keywords=Unknown%20ransomware%20operator&sort=relevance&index=ex&is_active=true

- (5) NSOPW – National Sex Offender Registry:

<https://www.nsopw.gov/Search/Results?firstName=&lastName=Unknown%20ransomware%20operator&city=&county=&state=0&zip=&radius=0>

- (6) BOP – Federal Inmate Locator: <https://www.bop.gov/inmateloc/>

- (7) FBI Most Wanted: <https://www.fbi.gov/wanted/search?q=Unknown%20ransomware%20operator>

- (8) FinCEN Enforcement Actions: <https://www.fincen.gov/news/enforcement-actions>





CONFIDENTIAL - AUTHORISED RECIPIENTS ONLY

(9) OFAC Sanctions List Search: <https://sanctionssearch.ofac.treas.gov/Details.aspx>

Financial Crime & Asset Tracing

(1) ACFE – Fraud Examiner Resources: <https://www.acfe.com/>

(2) FATF – Financial Action Task Force: <https://www.fatf-gafi.org/en/countries.html>

(3) OCCRP Aleph – Financial Crime Database:

<https://aleph.occrp.org/search?q=Unknown%20ransomware%20operator>

(4) StAR – Stolen Asset Recovery Initiative: <https://star.worldbank.org/>

SOURCES_UNAVAILABLE: Interpol Red Notices, ICIJ Offshore Leaks, Google News RSS, IP Geolocation (Domain Server), EU VIES VAT Registry





BLACKBOX

OPERATIONAL INTELLIGENCE

OPS-CKT5PZ

11 Oct 2026 · 19:53 UTC



CONFIDENTIAL — AUTHORISED RECIPIENTS ONLY



BLACKBOX

OPS-CKT5PZ · END OF REPORT

NEAR-ZERO RETENTION

This report was generated on demand and delivered once. It is not written to any database and is discarded from server memory 15 minutes after generation. Save this PDF in a secure location with access restricted to authorised recipients.

Generated: 11 Oct 2026 · 19:53 UTC

Reference: OPS-CKT5PZ

Classification: Confidential

[blackbox.fyi](#)