REDLab Product Security Newsletter

Cohesity REDLab is the data protection industry's only dedicated source of actionable intelligence on how malware interacts with backup infrastructure. This team of experts operates an air-gapped facility where live malware is executed against production-grade Cohesity DataProtect and Cohesity NetBackup deployments. By analyzing sophisticated malware, researchers gain deeper insight into emerging techniques and tactics. These findings help drive the design and enhancement of advanced threat detection and scanning technologies, strengthening defences against ransomware attacks.

This newsletter provides monthly updates on the most impactful ransomware strains evaluated in REDLab, along with comprehensive findings concerning detection and recovery procedures.

Cohesity DataProtect and NetBackup in REDLab

REDLab incorporates both Cohesity DataProtect and Cohesity NetBackup to conduct extensive testing against malware and sophisticated cyberattacks. Through live malware execution, real-world exploit detonation, and modern attack techniques, REDLab evaluates the performance of Cohesity solutions under authentic attack conditions. Its air-gapped environment enables comprehensive threat assessment in a controlled setting. REDLab testing is guided by the following principles:

- **Live, Current Threats:** Every strain detonated in REDLab is active malware sourced from real-world circulation - not synthetic samples or theoretical attack models - ensuring results reflect the threats security teams face today.
- **Production-Grade Conditions:** Tests are conducted on fully configured DataProtect and NetBackup deployments within an air-gapped facility designed to mirror real customer environments, rather than simplified lab setups.
- **Continuously Expanding Scope:** REDLab's threat library is updated monthly with newly identified ransomware families and attack techniques, ensuring testing evolves alongside the threat landscape.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

REDLab Findings

During this month, the malware strains listed below were intentionally detonated to evaluate product efficacy of Cohesity DataProtect and NetBackup.

Strain Details	SHA-256 Hash (link to more details on VirusTotal)
Name: Akira Family: Akira	67afa125bf8812cd943abed2ed56ed6e07853600ad609b40bdf9ad4141e612b4
Name: Qilin Family: Qilin (Agenda)	37546b811e369547c8bd631fa4399730d3bdaff635e744d83632b74f44f56cf6
Name: Majinahanashi Family: Majinahanashi Ransomware Group	98565754be5c8c6bf8e6bfd9c27405849dd055ac3b35e0a7076be4a649fc8bf1
Name: Black Basta Family: Black Basta	5d2204f3a20e163120f52a2e3595db19890050b2faa96c6cba6b094b0a52b0aa

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Akira Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Service Stop	T1489	Impact
Obfuscated Files or Information	T1027	Defense Evasion
Software Packing	T1027.002	Defense Evasion
Impair Defenses	T1562	Defense Evasion
Disable or Modify Tools	T1562.001	Defense Evasion
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Windows Service	T1543.003	Persistence, Privilege Escalation
OS Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
Credentials In Files	T1552.001	Credential Access
Credentials from Password Stores	T1555	Credential Access
Credentials from Web Browsers	T1555.003	Credential Access
Replication Through Removable Media	T1091	Initial Access, Lateral Movement
Application Layer Protocol	T1071	Command and Control
Data from Local System	T1005	Collection
System Owner/User Discovery	T1033	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery

Note: Above table contains a curated subset of techniques prioritized for monitoring and response.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Malware impact post execution

Akira was selected for this month's report as one of the most active ransomware operations in the current landscape. Open-source tracking attributes roughly 1,500 leak-site victims to the group since it emerged in 2023, including a record 84 disclosures in March 2026 alone, and ranks it second only to Qilin by volume for the first quarter of 2026. The ransom note recovered in this detonation explicitly asserts that backups were destroyed before encryption, making Akira a direct test of recovery resilience.

Akira is a 64-bit Windows PE console payload (approximately 570 KB). A static YARA match confirmed the Akira family, and the binary is packed, carrying an unknown PE section name.

Before encrypting, the sample performs light environmental checks. It queries the keyboard layout and system locale, checks its process token for administrator or Windows User Account Control (UAC) elevation status, queries the FIPS cryptography policy and installs a SetUnhandledExceptionFilter anti-debug hook. A date-expiration style check was also observed, in which the process exits shortly after reading the local time.

Encryption is fast and highly parallel. The strain systematically walks user directories with wildcards, binds a large number of files to I/O Completion Ports for asynchronous encryption and overwrites existing files. Every affected file is renamed with an “.iqoj” extension, and a single ransom note filename, “readme-asldkas”, is copied across multiple directories.

The sample also attempts to stop active services, a pattern commonly used to release file locks held by databases and backup agents, and creates an autorun.inf file to propagate through removable media. REDLab analysis recorded theft of private information from local browsers and HTTP requests carrying features characteristic of malware traffic, including a request to a commonly exploitable directory path. The ransom note claims that corporate data was exfiltrated and backups removed, offers a test decryption, threatens publication on the group’s blog and directs the victim to a Tor-based chat portal using a victim-specific access code, confirming a double-extortion posture.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

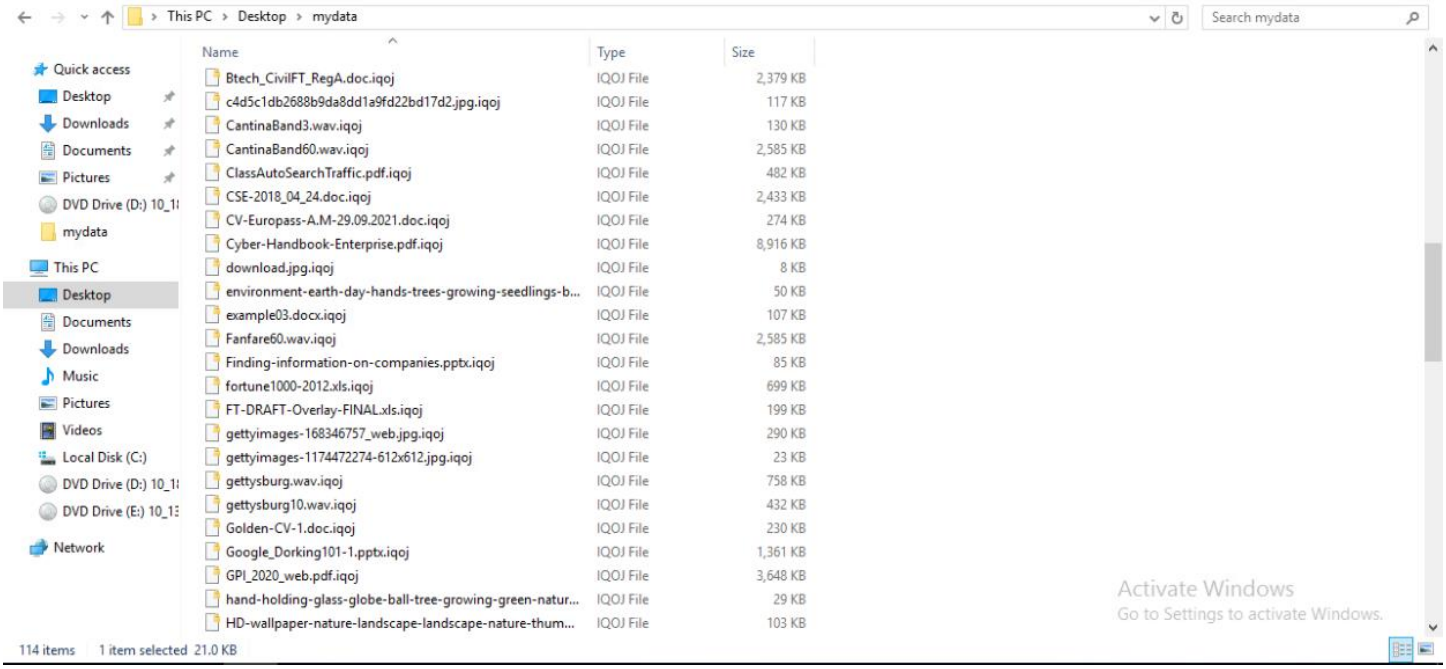


Figure 1: Victim files following detonation, each appended with the ".iqoj" extension.

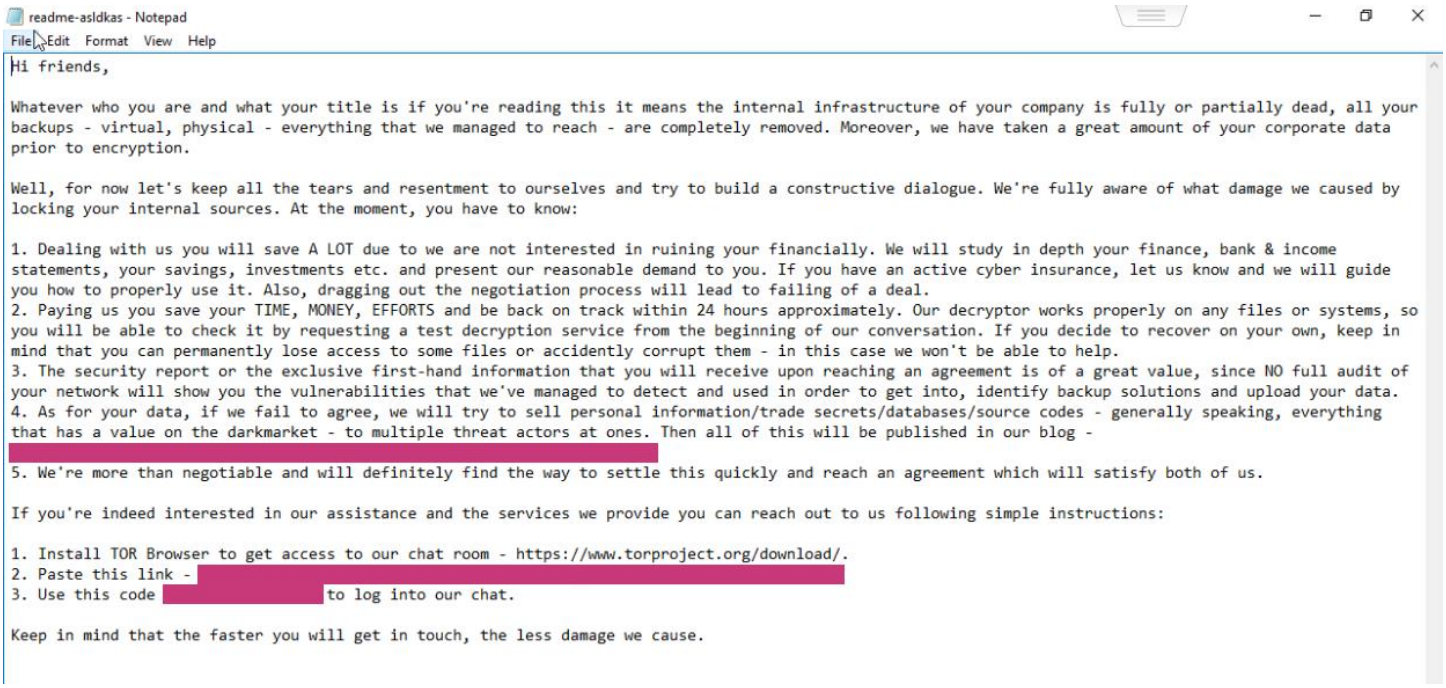


Figure 2: The "readme-asldkas" ransom note claiming data theft and backup destruction, with the Tor portal details redacted.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Protection & Detection Outcomes

Both DataProtect and NetBackup performed successful VMware backup and recovery following the attack. DataProtect VMware backup operations remained unaffected throughout. NetBackup's Image Entropy anomaly detection actively identified unusual deviation in VMware backup job attributes demonstrating its threat detection capabilities working as designed. VMware based backup and recovery was successful for both products.

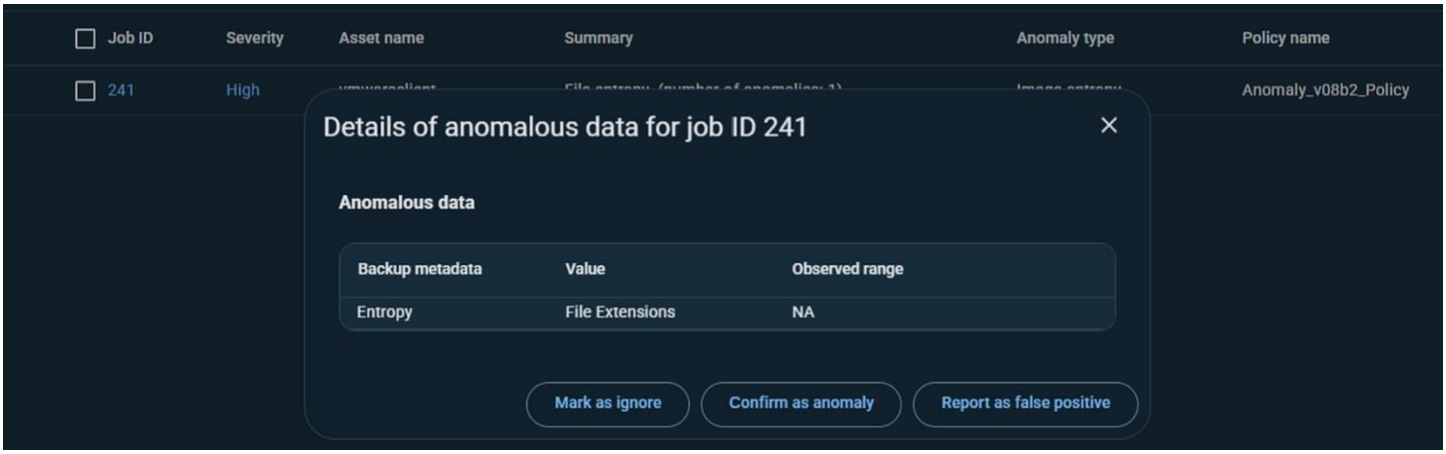


Figure 3: Akira NetBackup Entropy Anomaly Result.

Threat Hunting Results

Following the ransomware attack, Rapid Threat Hunt was leveraged to proactively search for malicious activity using known SHA-256 hash and IOC associated with the Akira ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

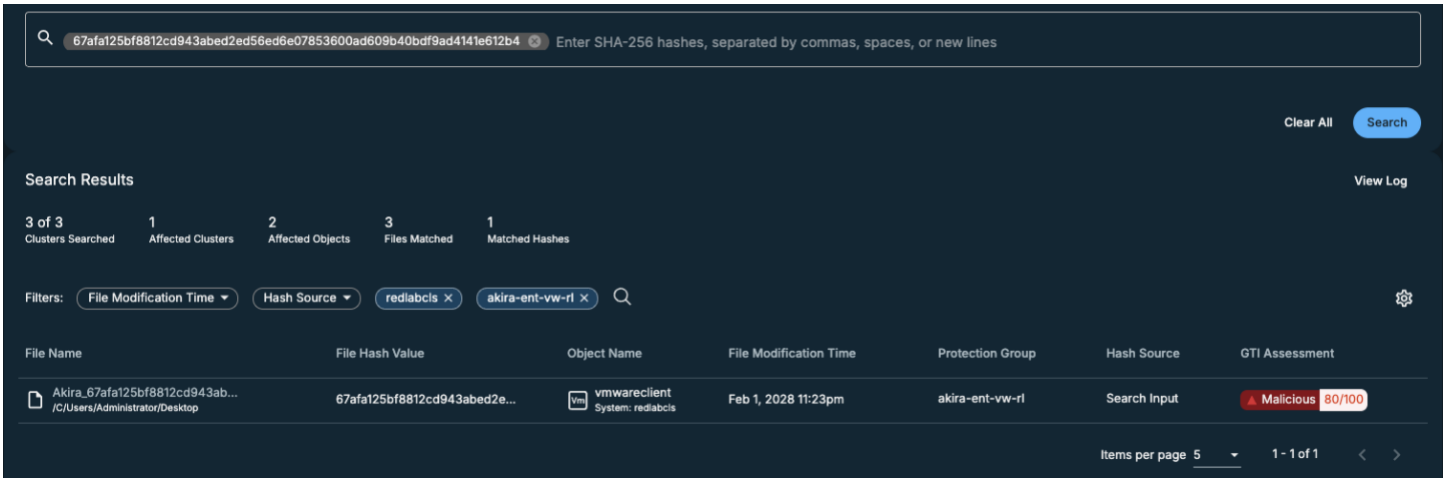


Figure 4: Akira Rapid Threat Hunt Result.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Qilin Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Service Stop	T1489	Impact
Inhibit System Recovery	T1490	Impact
Obfuscated Files or Information	T1027	Defense Evasion
Process Injection	T1055	Defense Evasion, Privilege Escalation
Indicator Removal	T1070	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Impair Defenses	T1562	Defense Evasion
Hijack Execution Flow	T1574	Defense Evasion, Execution
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Command and Scripting Interpreter	T1059	Execution
Native API	T1106	Execution
Shared Modules	T1129	Execution
System Services	T1569	Execution
Input Capture	T1056	Collection, Credential Access
Application Layer Protocol	T1071	Command and Control
Proxy	T1090	Command and Control
Archive Collected Data	T1560	Collection
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Network Share Discovery	T1135	Discovery
Software Discovery	T1518	Discovery

Note: Above table contains a curated subset of techniques prioritized for monitoring and response.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Malware impact post execution

According to our research, Qilin was the most active ransomware group of 2026 to date. Open-source tracking shows about 100 leak-site listings per month on average. The group hit a record of at least 165 incidents in August 2026. It has been the leading ransomware operation since the second quarter of 2025. Its affiliate model has also reportedly seeded newer brands, including The Gentlemen, which was evaluated in last month's edition.

Qilin (also tracked as Agenda) is a 32-bit Windows PE console payload (approximately 1.6 MB) that requires an operator-supplied "-password" argument to run. Static analysis matched multiple YARA rules and showed a thread-local-storage section, a registered vectored exception handler and a SetUnhandledExceptionFilter hook, consistent with anti-analysis and execution-flow hijacking.

When launched with the password argument, the sample prints a 45-second pre-encryption notification and then turns to service manipulation. It attempted to stop or disable BrokerInfrastructure, ClipSVC, gpsvc, NgcCtnrSvc, RmSvc, SamSs, tiledatamodelsvc, TimeBrokerSvc, VSS, WinDefend and wudfsvc. Several calls failed with access-denied errors, but the Volume Shadow Copy service and several others were stopped and disabled, and an explicit attempt to remove shadow copies failed with a non-zero exit code.

Encryption runs in global traversal mode across local and attached volumes. In this detonation the sample encrypted 5,457 files in roughly 31 seconds, appending a randomly generated ten-character extension (".gBBQsRxAcQ") and writing a "README-RECOVER" ransom note named with the same identifier into each directory; repeated "file exists" errors confirm the note was already present in many folders. Files that could not be opened were skipped with "can't open file" warnings.

The ransom note claims that sensitive data was downloaded, listing employee personal data, a complete network map with credentials, financial records and manufacturing schematics. It warns that modifying files or using third-party recovery tools will prevent decryption, states that police or authorities cannot help recover the key and directs the victim to a Tor-hosted portal using victim-specific credentials, confirming a double-extortion posture.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

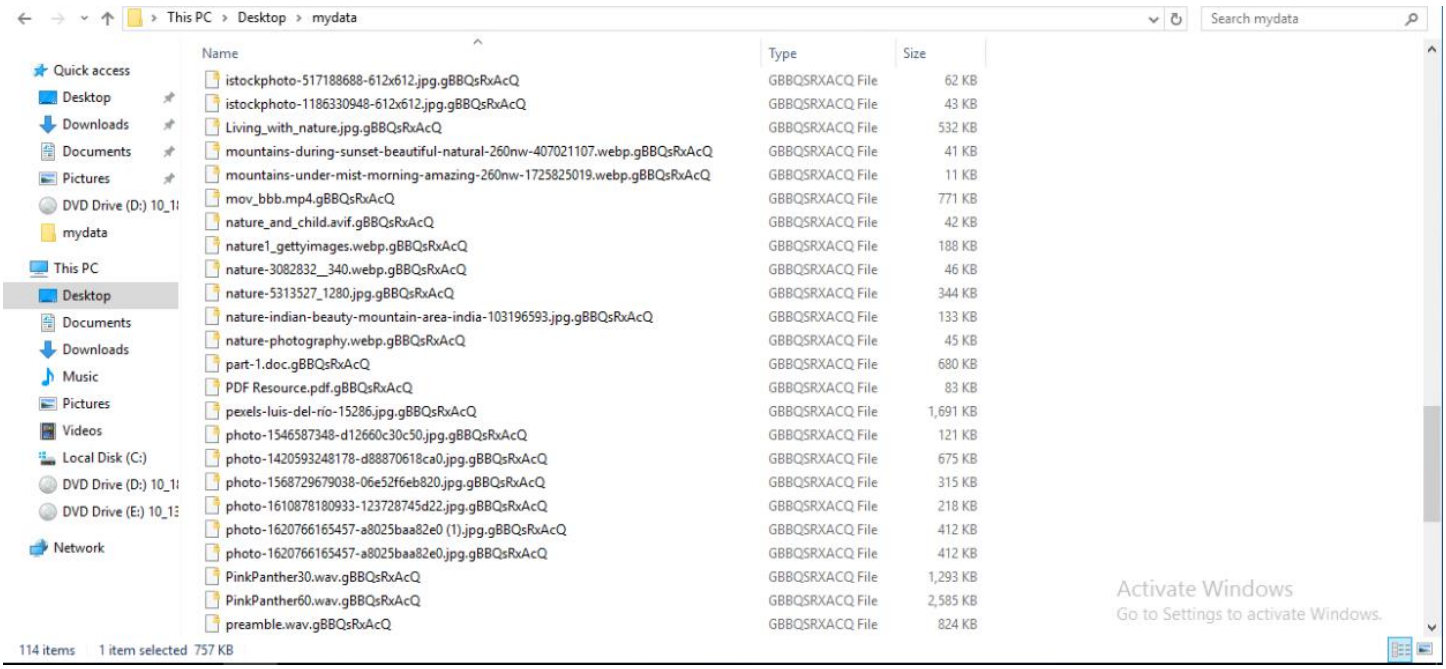
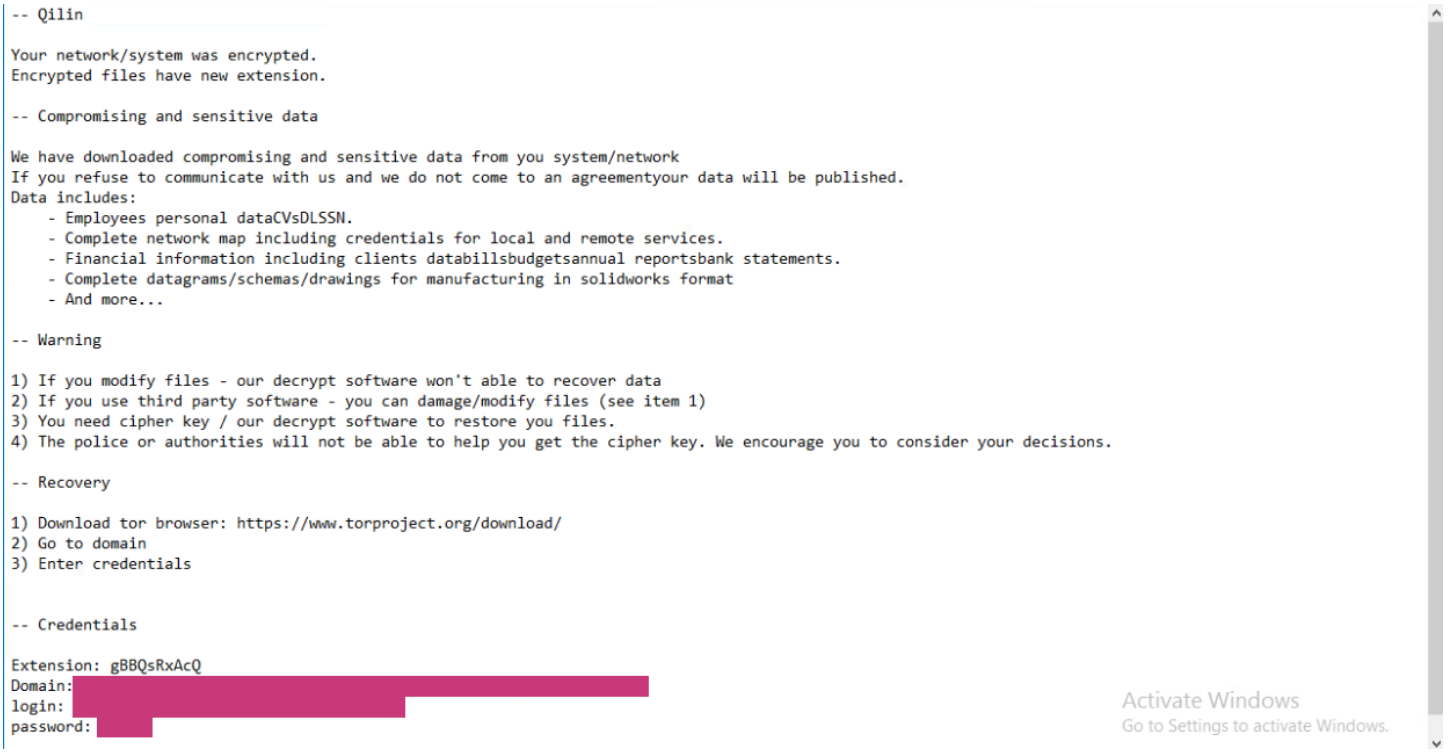


Figure 5: Victim files following detonation, each appended with the ".gBBQsRxAcQ" extension.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.



```
-- Qilin

Your network/system was encrypted.
Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from you system/network
If you refuse to communicate with us and we do not come to an agreementyour data will be published.
Data includes:
    - Employees personal dataCVsDLSSN.
    - Complete network map including credentials for local and remote services.
    - Financial information including clients databillsbudgetsannual reportsbank statements.
    - Complete datagrams/schemas/drawings for manufacturing in solidworks format
    - And more...

-- Warning

1) If you modify files - our decrypt software won't able to recover data
2) If you use third party software - you can damage/modify files (see item 1)
3) You need cipher key / our decrypt software to restore you files.
4) The police or authorities will not be able to help you get the cipher key. We encourage you to consider your decisions.

-- Recovery

1) Download tor browser: https://www.torproject.org/download/
2) Go to domain
3) Enter credentials


-- Credentials

Extension: gBBQsRxAcQ
Domain: [redacted]
login: [redacted]
password: [redacted]
```

Activate Windows
Go to Settings to activate Windows.

Figure 6: The "README-RECOVER" ransom note claiming data theft and listing the stolen data categories, with the Tor portal credentials redacted.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Protection & Detection Outcomes

Both DataProtect and NetBackup performed successful VMware backup and recovery following the attack. DataProtect VMware backup operations remained unaffected throughout. NetBackup's Image Entropy anomaly detection actively identified unusual deviation in VMware backup job attributes demonstrating its threat detection capabilities working as designed. VMware based backup and recovery was successful for both products.

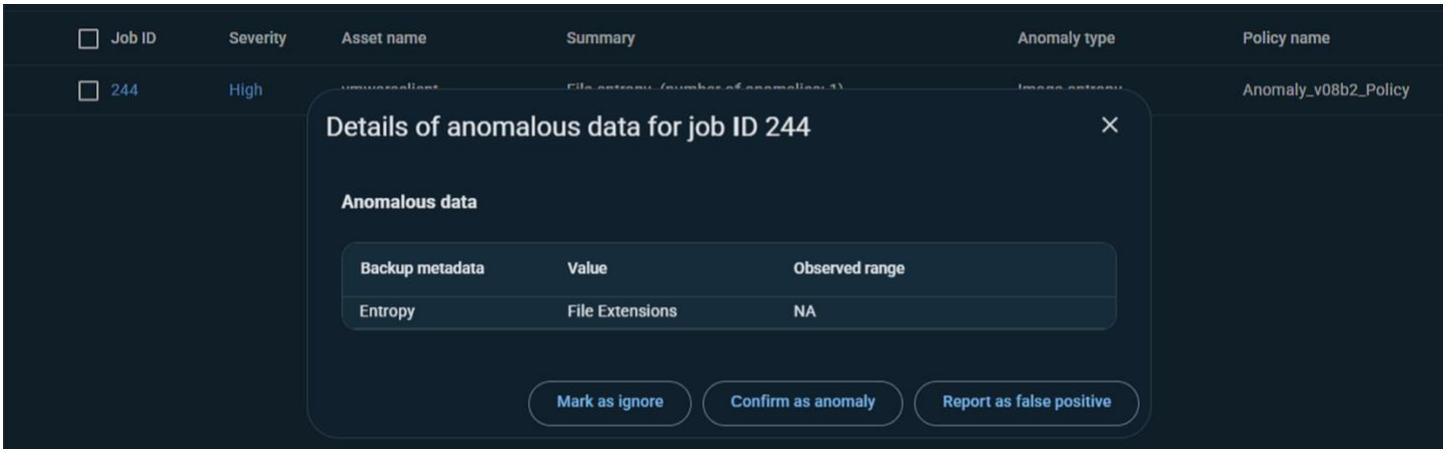


Figure 7: Qilin NetBackup Entropy Anomaly Result.

Threat Hunting Results

Following the ransomware attack, Rapid Threat Hunt was leveraged to proactively search for malicious activity using known SHA-256 hash and IOC associated with the Qilin ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

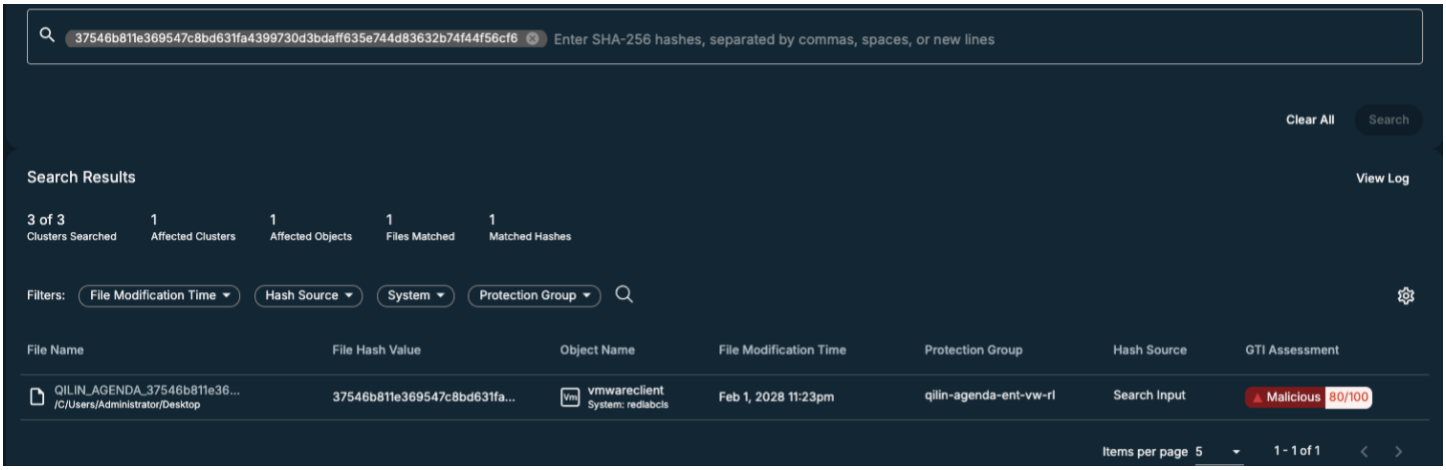


Figure 8: Qilin Rapid Threat Hunt Result.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Majinahanashi Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Destruction	T1485	Impact
Data Encrypted for Impact	T1486	Impact
Service Stop	T1489	Impact
Inhibit System Recovery	T1490	Impact
Indicator Removal	T1070	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Bootkit	T1542.003	Defense Evasion, Persistence
Impair Defenses	T1562	Defense Evasion
Disable or Modify Tools	T1562.001	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Windows Service	T1543.003	Persistence, Privilege Escalation
Command and Scripting Interpreter	T1059	Execution
Application Layer Protocol	T1071	Command and Control
System Owner/User Discovery	T1033	Discovery
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery

Note: Above table contains a curated subset of techniques prioritized for monitoring and response.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Malware impact post execution

Majinahanashi was selected as an emerging double-extortion group first observed in mid-2026. Open-source reporting dates its first activity to between July and August 2026. It credits the group with roughly 40 claimed victims so far. Counts vary by tracker. The victims include hospitality, e-commerce, manufacturing, construction, and engineering firms located in the United Kingdom, Europe, Malaysia, and the United States.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

The group reportedly rebranded its leak site on October 2, 2026, indicating active and continuing development.

Majinahanashi is a compact 64-bit Windows PE payload (GUI subsystem, approximately 90 KB). Despite its small size, the payload carries an extensive pre-encryption routine.

Before encrypting, the sample profiles the host extensively. It queries the keyboard layout, system locale, language registry key, computer name and available memory, enumerates services and running processes (expressing interest in specific processes) and reads the volume serial number and physical hardware ID for victim profiling. It also checks its token for administrator or UAC elevation status, queries the FIPS cryptography policy, resolves functions dynamically, uses a mutex for inter-process synchronization and installs a SetUnhandledExceptionFilter anti-debug hook. A date-expiration check was observed, and the process created a hidden window to keep the activity off-screen.

Encryption is broad and destructive. The payload uses Restart Manager sessions to release locked files, performs a large number of encryption calls using the same key, and REDLab analysis recorded mass file deletion and overwriting of existing files. Every affected file is renamed with a ".majin" extension, and a single ransom note filename, "README", is copied across multiple directories.

Anti-recovery is thorough. The sample attempts to stop active services, modifies boot configuration through bcdedit, deletes or modifies volume shadow copies, clears Windows event logs and issues suspicious IO control codes consistent with disk enumeration or bootkit and wiper behavior, while using Windows utilities to carry out parts of the routine indirectly. The ransom note asserts that backups and shadow copies were removed and that internal data was extracted, offers to decrypt two files as proof, directs contact through qTOX and email and sets a seven-day deadline before the full dataset is released on a Tor disclosure site.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

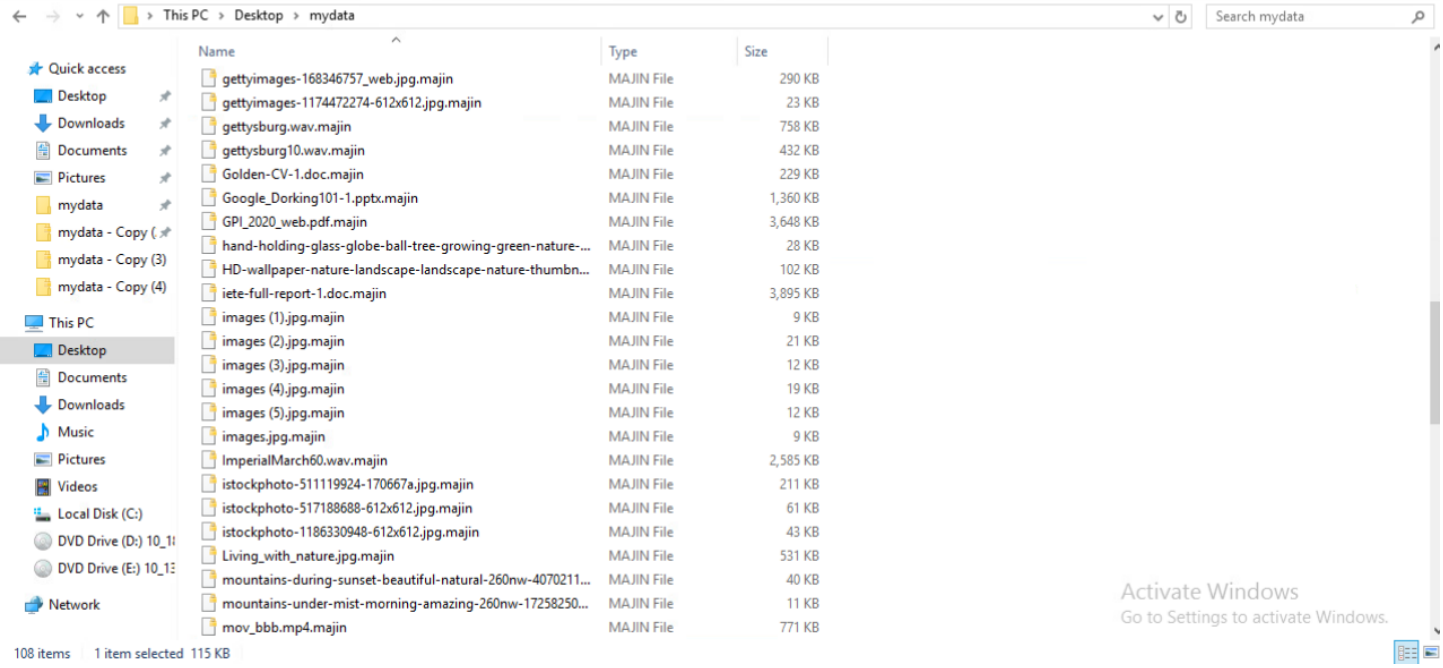
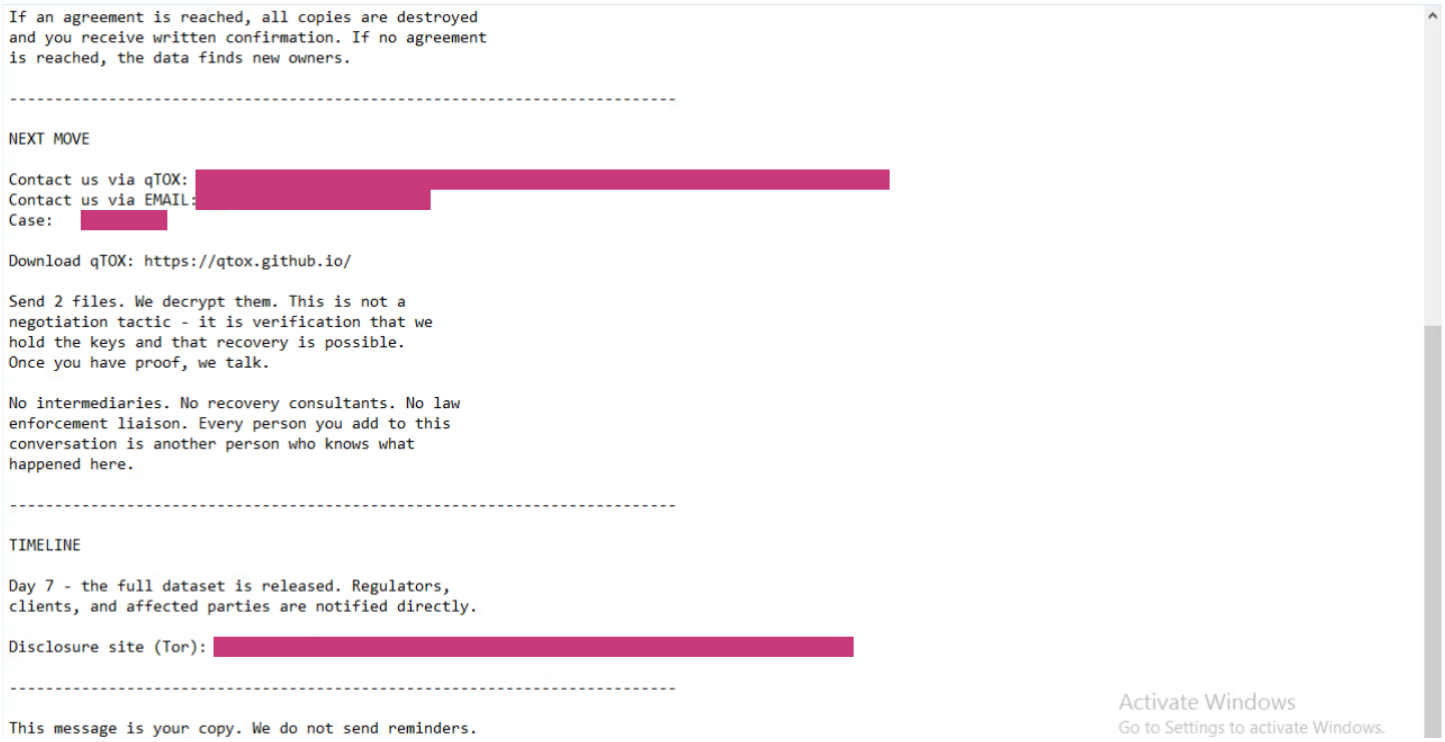


Figure 9: Victim files following detonation, each appended with the ".majin" extension.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.



```
If an agreement is reached, all copies are destroyed
and you receive written confirmation. If no agreement
is reached, the data finds new owners.

--------------------------------------------------------------------------

NEXT MOVE

Contact us via qTOX: [redacted]
Contact us via EMAIL: [redacted]
Case:   [redacted]

Download qTOX: https://qtox.github.io/

Send 2 files. We decrypt them. This is not a
negotiation tactic - it is verification that we
hold the keys and that recovery is possible.
Once you have proof, we talk.

No intermediaries. No recovery consultants. No law
enforcement liaison. Every person you add to this
conversation is another person who knows what
happened here.

--------------------------------------------------------------------------

TIMELINE

Day 7 - the full dataset is released. Regulators,
clients, and affected parties are notified directly.

Disclosure site (Tor): [redacted]

--------------------------------------------------------------------------

This message is your copy. We do not send reminders.
```

Activate Windows
Go to Settings to activate Windows.

Figure 10: The "README" ransom note listing the verification offer, seven-day disclosure timeline and Tor disclosure site, with contact details redacted.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Protection & Detection Outcomes

Both DataProtect and NetBackup performed successful VMware backup and recovery following the attack. DataProtect VMware backup operations remained unaffected throughout. NetBackup's Image Entropy anomaly detection actively identified unusual deviation in VMware backup job attributes demonstrating its threat detection capabilities working as designed. VMware based backup and recovery was successful for both products.

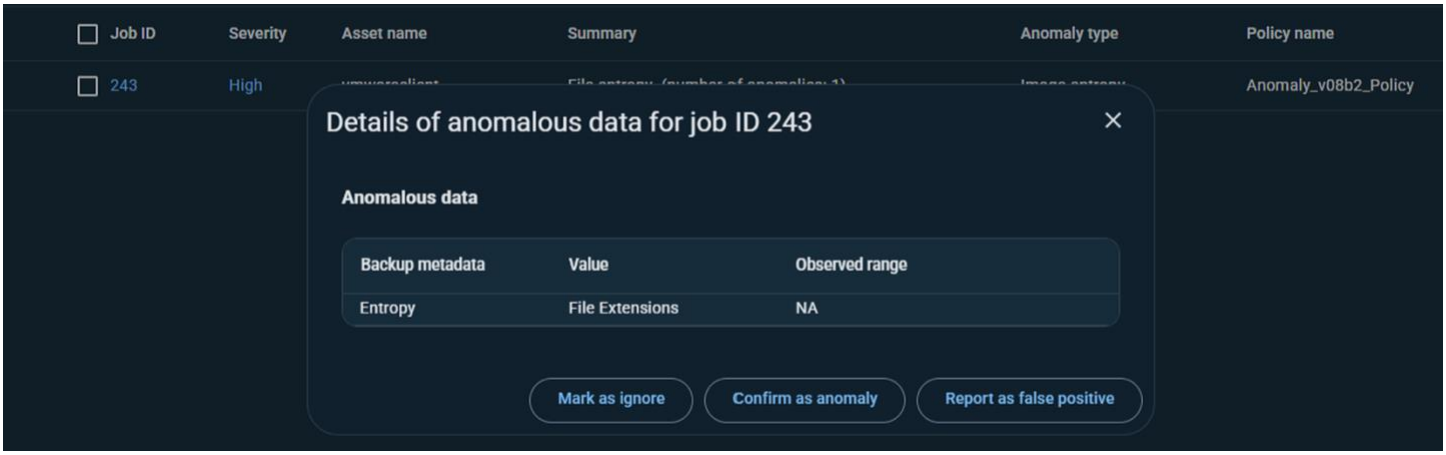


Figure 11: Majinahanashi NetBackup Entropy Anomaly Result.

Threat Hunting Results

Following the ransomware attack, Rapid Threat Hunt was leveraged to proactively search for malicious activity using known SHA-256 hash and IOC associated with the Majinahanashi ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

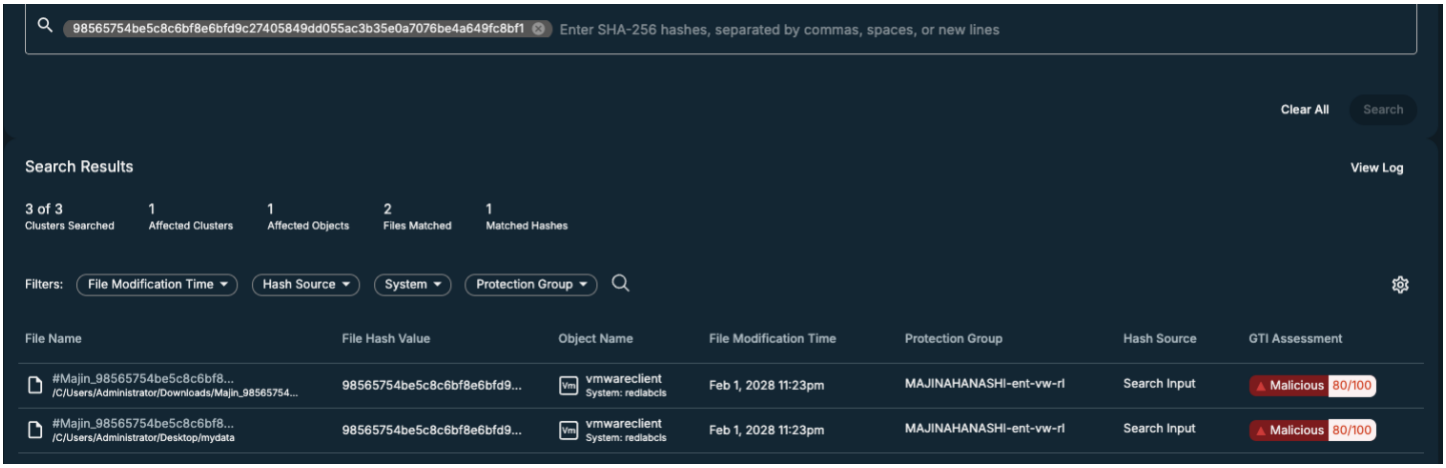


Figure 12: Majinahanashi Rapid Threat Hunt Result.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Black Basta Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Masquerading	T1036	Defense Evasion
Modify Registry	T1112	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Hide Artifacts	T1564	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Scheduled Task/Job	T1053	Persistence, Privilege Escalation, Execution
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Windows Service	T1543.003	Persistence, Privilege Escalation
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Registry Run Keys / Startup Folder	T1547.001	Persistence, Privilege Escalation
Command and Scripting Interpreter	T1059	Execution
Application Layer Protocol	T1071	Command and Control
Data Staged	T1074	Collection
System Owner/User Discovery	T1033	Discovery
System Information Discovery	T1082	Discovery

Note: Above table contains a curated subset of techniques prioritized for monitoring and response.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Malware impact post execution

Black Basta is a 32-bit Windows PE console payload (approximately 560 KB).

The sample performs several anti-analysis and profiling checks before encrypting. It checks for mouse movement and available memory, queries the keyboard layout, locale and language registry key, reads the volume serial number and physical hardware ID, queries the FIPS cryptography policy and checks its token for administrator or UAC elevation status. It enumerates mount points and registry mount points to identify local, removable and network drives, reads the memory of another process, creates a hidden window, runs commands with the /C switch so the shell terminates on completion and installs a SetUnhandledExceptionFilter anti-debug hook. A date-expiration check was also observed.

Persistence is established through several mechanisms in parallel: autorun at Windows startup, a scheduled task and a service that was created but not started. Boot configuration is modified through bcdedit, volume shadow copies are deleted or modified, and the sample attempted to restart the guest machine, behavior associated with anti-sandbox restarts and recovery-resistant reboots.

Impact is branded and visible. Registry keys are modified for file-extension hijacking so that encrypted files receive a custom “.basta” type and icon, the Recycle Bin is manipulated, and the desktop wallpaper is replaced with a notice that the network is encrypted by the Black Basta group and that instructions are in “readme.txt”. The note claims data was stolen and encrypted, threatens publication on a Tor leak site, offers free decryption of one file and supplies a victim-specific company identifier. The sample also issued HTTP requests with features characteristic of malware traffic, including a request to a commonly exploitable directory path.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

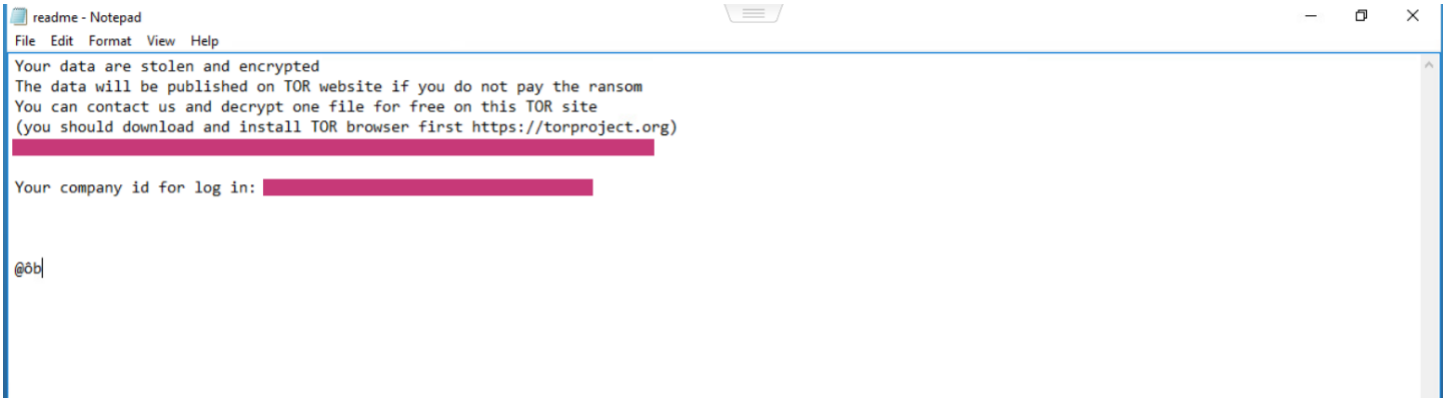


Figure 13: The "readme" ransom note claiming data theft and encryption, with the Tor portal address and company identifier redacted.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.



Figure 14: Desktop wallpaper replaced after encryption with a notice that the network is encrypted by the Black Basta group.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Protection & Detection Outcomes

Both DataProtect and NetBackup performed successful VMware backup and recovery following the attack. DataProtect VMware backup operations remained unaffected throughout. NetBackup's Image Entropy anomaly detection actively identified unusual deviation in VMware backup job attributes demonstrating its threat detection capabilities working as designed. VMware based backup and recovery was successful for both products.

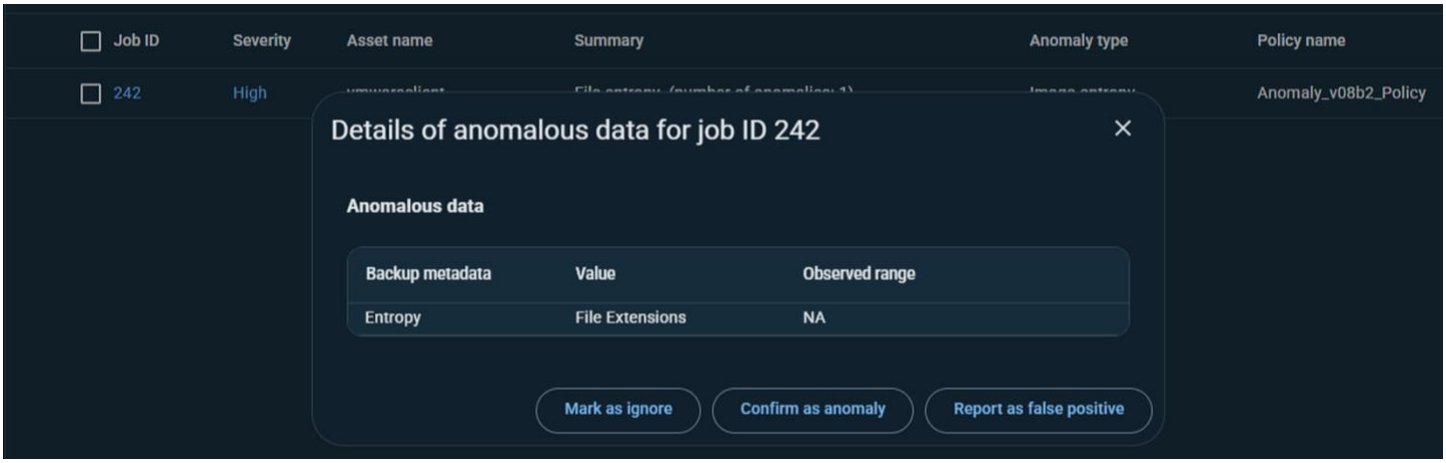


Figure 15: Black Basta NetBackup Entropy Anomaly Result.

Threat Hunting Results

Following the ransomware attack, Rapid Threat Hunt was leveraged to proactively search for malicious activity using known SHA-256 hash and IOC associated with the Black Basta ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

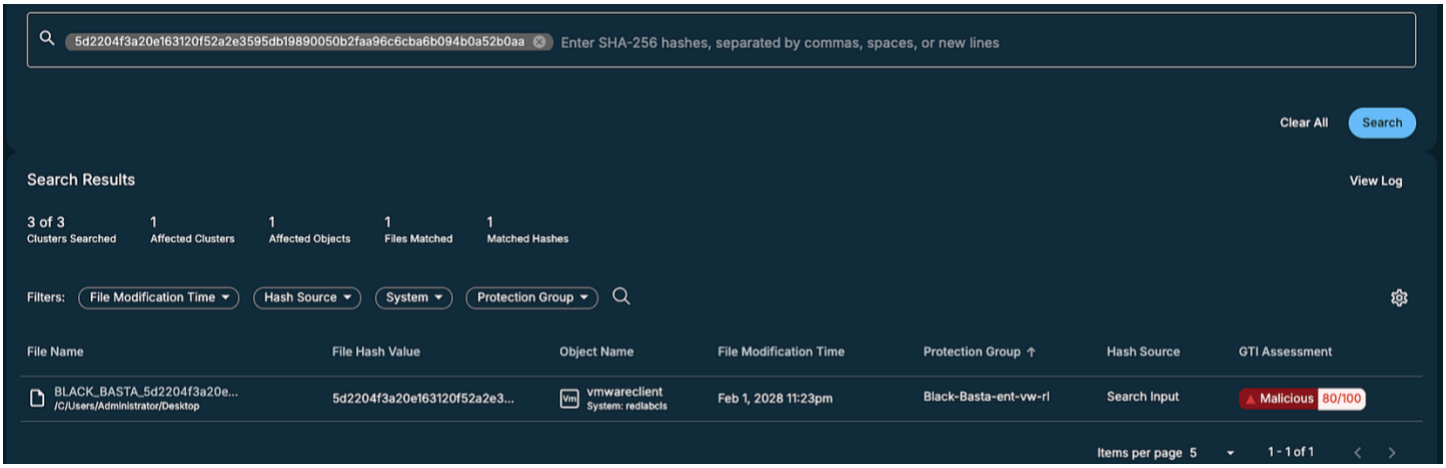


Figure 16: Black Basta Rapid Threat Hunt Result.

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.

Summary

- Both DataProtect and NetBackup achieved successful VMware backup and recovery across all four ransomware strains tested this month – Akira, Qilin, Majinahanashi and Black Basta, demonstrating the resilience of Cohesity's solutions under real-world attack conditions.

- DataProtect VMware backup operations remained unaffected throughout all tests, validating the platform's ability to maintain data protection under adverse conditions.

- NetBackup's Image Entropy anomaly detection actively identified unusual deviations in VMware backup job attributes - confirming its active threat detection capabilities working as designed. VMware based backup and recovery was successful.

- Rapid Threat Hunt enabled proactive threat investigation by correlating known malicious SHA-256 hashes and IOCs against protected environments, successfully identifying impacted clusters, objects and file artifacts.

For more information on REDLab please visit https://cohesity.com/redlab

© 2026 Cohesity, Inc. All rights reserved. Cohesity, the Cohesity logo, SnapTree, SpanFS, DataPlatform, DataProtect, Helios, and other Cohesity marks are trademarks or registered trademarks of Cohesity, Inc. in the US and/or internationally. Other company and product names may be trademarks of the respective companies with which they are associated.