REDLab Product Security Newsletter

Cohesity REDLab is a fully isolated security testing environment, hosted and managed by Cohesity, designed for comprehensive malware research and analysis. Within REDLab, live malware is executed to rigorously stress test Cohesity solutions, ensuring that products are resilient against real-world cyber threats. This process enhances the understanding of effective data protection and security methodologies. The insights gained provide valuable guidance to both security and data protection teams, reinforcing confidence in data safety and the cyber resilience offered by Cohesity solutions.

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 platforms to enable extensive testing against malware and sophisticated cyberattacks. Through live malware execution, advanced exploit simulation, and modern attack techniques, REDLab examines the practical robustness of Cohesity's solutions. The air-gapped nature of REDLab ensures comprehensive threat assessment under controlled conditions.

- **Proven Confidence:** Backup and recovery solutions undergo rigorous validation against active, high-level cyber threats, not just theoretical threats or synthetic data.
- **Hardened Defense:** Testing in REDLab verifies that DataProtect and NetBackup offer strong security capabilities, elevating them beyond standard recovery tools to proactive defense mechanisms.
- **Future-Ready:** REDLab continually broadens its testing scope to encompass advanced threat detection and threat hunting, ensuring ongoing adaptability and resilience in response to evolving threats.

REDLab Findings

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

Strain Details	Hash / IOC
Name: Direwolf Family: DireWolf Hacking Group	8fdee53152ec985ffeeeda3d7a85852eb5c9902d2d480449421b4939b1904aad
Name: HelloKitty Family: HelloKitty Malware Family	9a7daafc56300bd94ceef23eac56a0735b63ec6b9a7a409fb5a9b63efe1aa0b0
Name: KaWaLocker Family: KawaLocker Ransomware Family	f3a6d4ccdd0f663269c3909e74d6847608b8632fb2814b0436a4532b8281e617
Name: Lockis Family: Locky Ransomware Family	f3741203fb8b0daa627d0b9f52a33a75cf42eb1c5142a398185af58d9ed36ded

Direwolf Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Windows Management Instrumentation	T1047	Execution
Command and Scripting Interpreter	T1059	Execution
Scripting	T1064	Execution, Defense Evasion
Native API	T1106	Execution
Shared Modules	T1129	Execution
System Services	T1569	Execution
Server Software Component	T1505	Persistence
Pre-OS Boot	T1542	Persistence, Defense Evasion
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Hijack Execution Flow	T1574	Persistence, Privilege Escalation, Defense Evasion
Process Injection	T1055	Privilege Escalation, Defense Evasion
Rootkit	T1014	Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Impair Defenses	T1562	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
Application Window Discovery	T1010	Discovery

Malware impact post execution

Direwolf encrypted user and system data, renaming each file with **“.direwolf”** extension. It dropped **README.TXT** as its ransom note and actively killed processes holding open database, document and productivity files to maximize encryption coverage. BackLock is commonly delivered through phishing, drive-by downloads and RDP brute-force attacks. It has also been observed in campaigns abusing vulnerabilities in MOVEit Transfer and Citrix NetScaler environments.

Image: Files encrypted post attack with “.direwolf” extension.

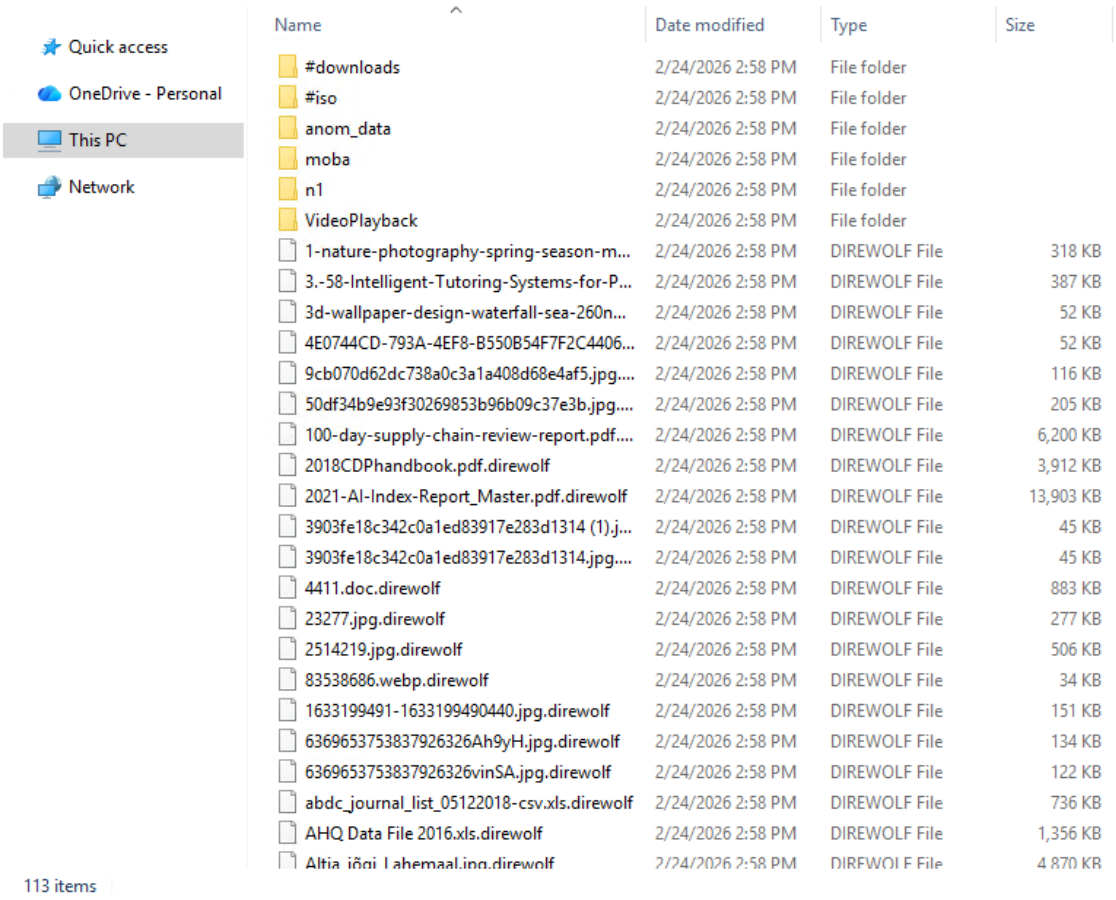
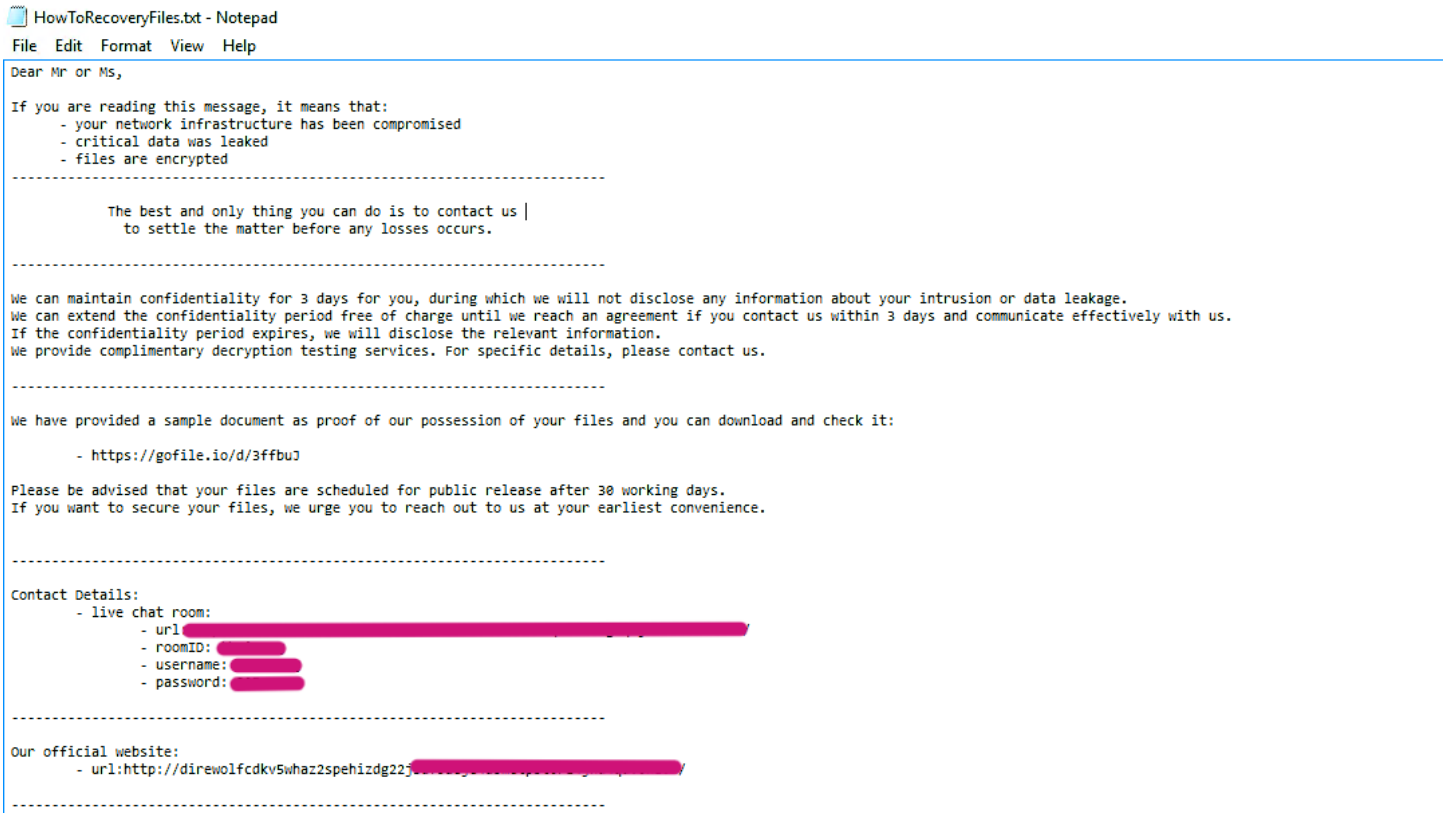


Image: Ransom Note named "HowToRecoveryFiles.txt" dropped along with recovery details.



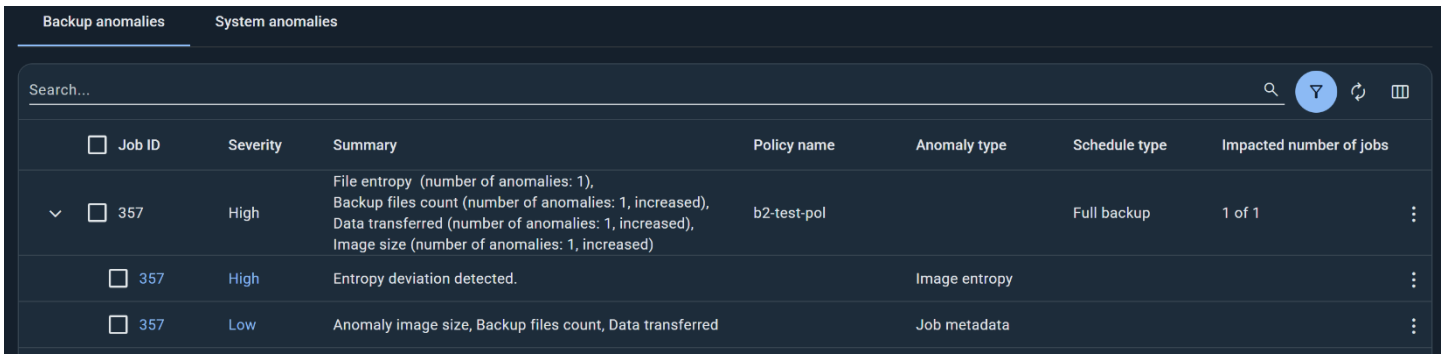
HowToRecoveryFiles.txt - Notepad

File Edit Format View Help

```
Dear Mr or Ms,

If you are reading this message, it means that:
      - your network infrastructure has been compromised
      - critical data was leaked
      - files are encrypted
-------------------------------------------------------------------------

            The best and only thing you can do is to contact us
              to settle the matter before any losses occurs.

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

We can maintain confidentiality for 3 days for you, during which we will not disclose any information about your intrusion or data leakage.
We can extend the confidentiality period free of charge until we reach an agreement if you contact us within 3 days and communicate effectively with us.
If the confidentiality period expires, we will disclose the relevant information.
We provide complimentary decryption testing services. For specific details, please contact us.

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

We have provided a sample document as proof of our possession of your files and you can download and check it:

        - https://gofile.io/d/3ffbuJ

Please be advised that your files are scheduled for public release after 30 working days.
If you want to secure your files, we urge you to reach out to us at your earliest convenience.


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

Contact Details:
        - live chat room:
                - url[redacted]
                - roomID: [redacted]
                - username: [redacted]
                - password: [redacted]

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

Our official website:
        - url:http://direwolfcdkv5whaz2spehizdg22j[redacted]

-------------------------------------------------------------------------
```

Protection & Detection Outcomes

After the attack, the DataProtect Agent backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.



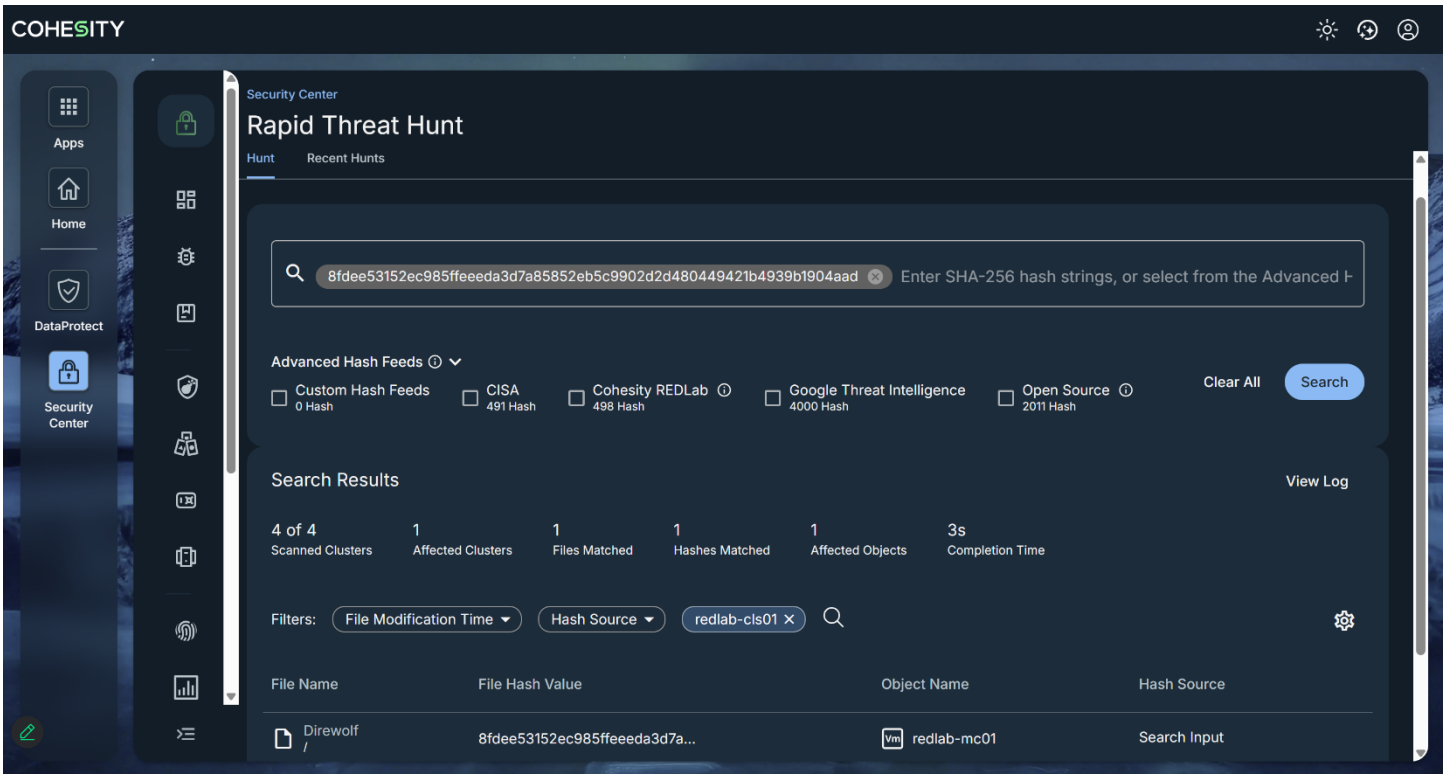
Backup anomalies | System anomalies

Search...

Job ID	Severity	Summary	Policy name	Anomaly type	Schedule type	Impacted number of jobs
357	High	File entropy (number of anomalies: 1), Backup files count (number of anomalies: 1, increased), Data transferred (number of anomalies: 1, increased), Image size (number of anomalies: 1, increased)	b2-test-pol		Full backup	1 of 1
357	High	Entropy deviation detected.		Image entropy		
357	Low	Anomaly image size, Backup files count, Data transferred		Job metadata		

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 Direwolf ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.



This capability enables security teams to quickly pivot from detection to investigation, validate threat presence, and assess potential blast radius across protected workloads.

HelloKitty Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Windows Management Instrumentation	T1047	Execution
Shared Modules	T1129	Execution
Inter-Process Communication	T1559	Execution
Boot or Logon Autostart Execution	T1547	Persistence
Hijack Execution Flow	T1574	Persistence, Privilege Escalation
Process Injection	T1055	Privilege Escalation, Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal	T1070	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Process Discovery	T1057	Discovery
Security Software Discovery	T1063	Discovery
Software Discovery	T1518	Discovery
Data Encrypted for Impact	T1486	Impact

Malware impact post execution

HelloKitty ransomware is a targeted crypto-ransomware family that focuses primarily on Windows environments, encrypting victim data and appending the **“.crypted”** extension to affected files, followed by the creation of a ransom note such as **“read_me_lkdtt.txt.”** HelloKitty ransomware has re-emerged in 2025 as an active threat after periods of relative inactivity, signalling a revival of the operation. Previously linked to high-profile enterprise breaches, the group appears to have resumed campaigns with refined tooling and a continued emphasis on disrupting corporate networks.

Image: Files encrypted post attack with “.crypted” extension.

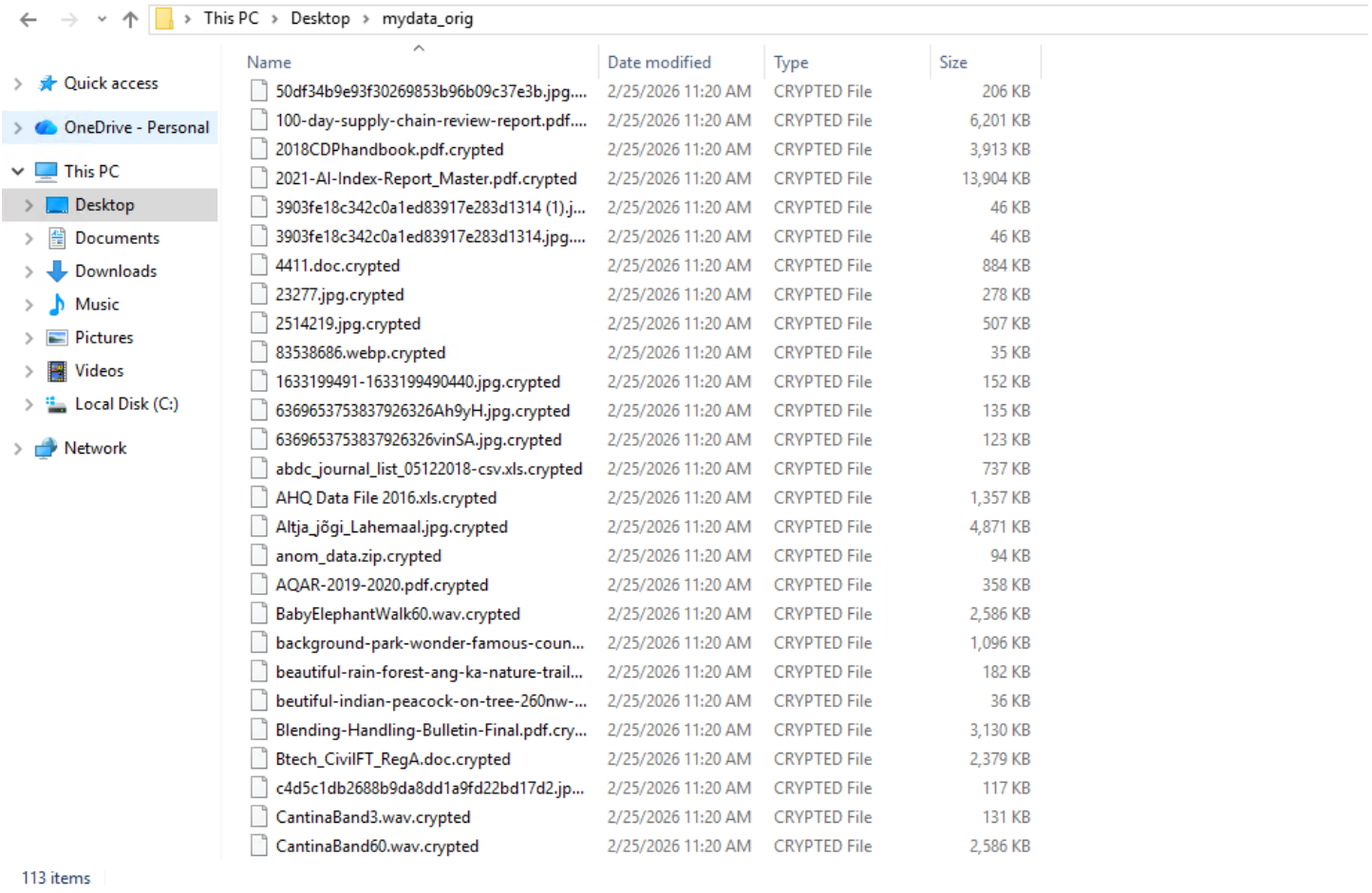
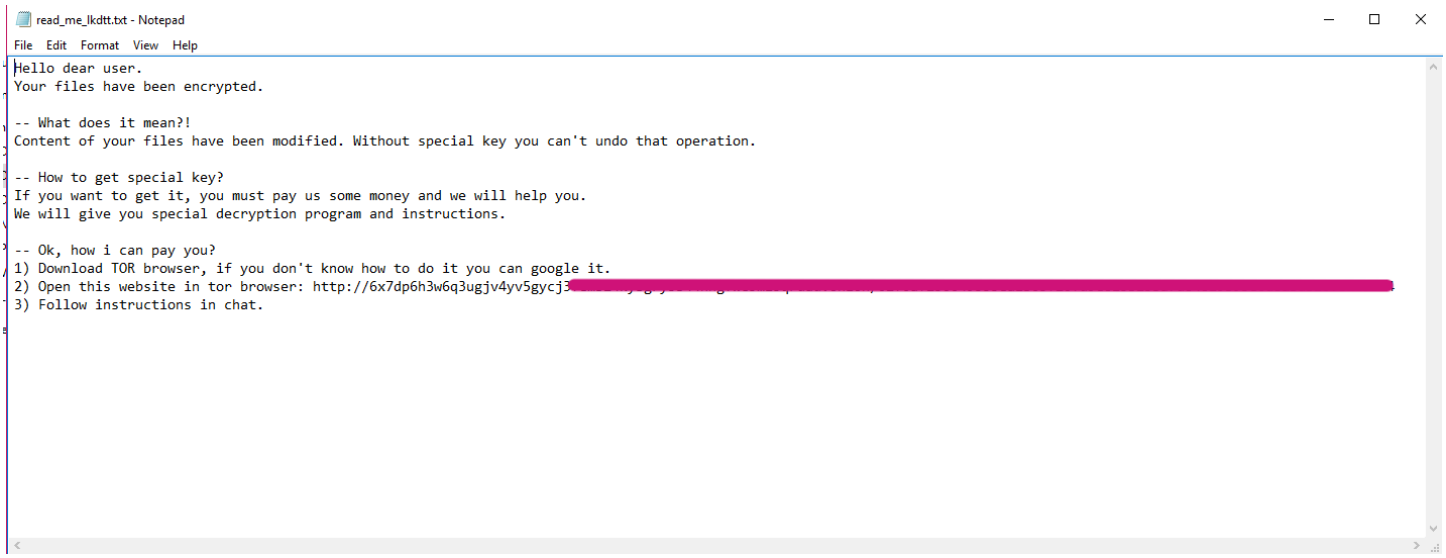
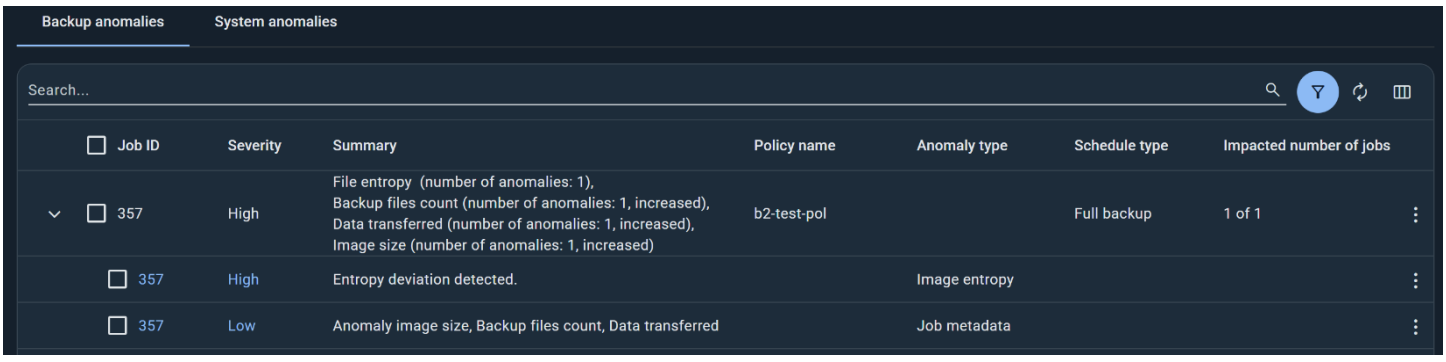


Image: Ransom Note named "read_me_lkdtt.txt" dropped along with recovery details.



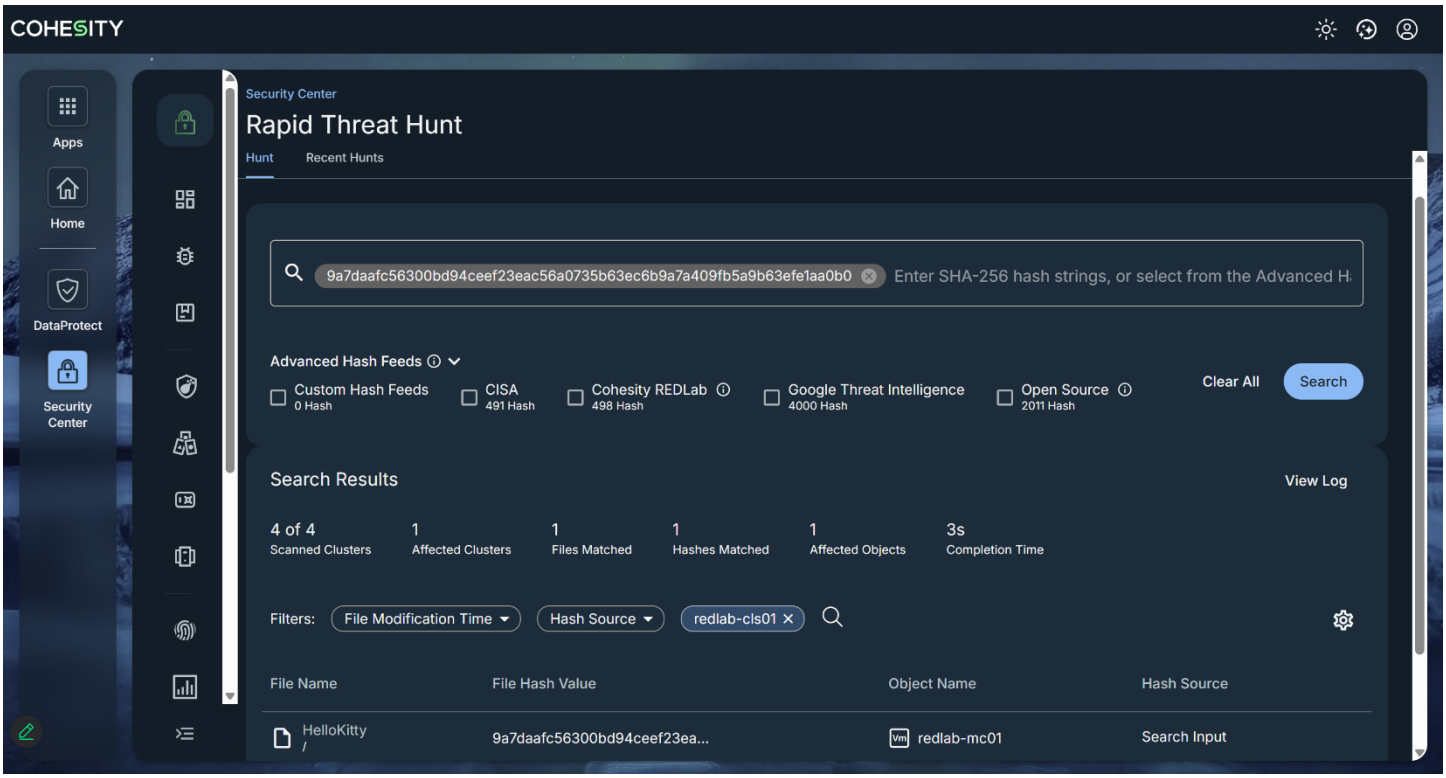
Protection & Detection Outcomes

After the attack, the DataProtect Agent backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.



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 HelloKitty ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.



This capability enables security teams to quickly pivot from detection to investigation, validate threat presence, and assess potential blast radius across protected workloads.

KawaLocker Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Windows Management Instrumentation	T1047	Execution
Shared Modules	T1129	Execution
Boot or Logon Autostart Execution	T1547	Persistence
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Pre-OS Boot	T1542	Persistence, Defense Evasion
Process Injection	T1055	Privilege Escalation, Defense Evasion
Access Token Manipulation	T1134	Privilege Escalation, Defense Evasion
Abuse Elevation Control Mechanism	T1548	Privilege Escalation, Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
Rootkit	T1014	Defense Evasion
System Information Discovery	T1082	Discovery
Process Discovery	T1057	Discovery
File and Directory Discovery	T1083	Discovery
System Service Discovery	T1007	Discovery
Data Encrypted for Impact	T1486	Impact
Data Destruction	T1485	Impact
Inhibit System Recovery	T1490	Impact

Malware impact post execution

KawaLocker ransomware is a Windows-targeting crypto-malware strain that executes its payload, enumerates local and network-accessible drives, and encrypts files using strong cryptographic routines. In our case, encrypted files were observed with the extension **.C3680868C** appended to their original names. The malware drops a ransom note titled **"!!Restore-My-file-Kavva.txt,"** stating that data has been encrypted and exfiltrated. Observed behavior is consistent with double-extortion technique, where attackers combine file encryption with data theft to increase pressure on the victim.

Image: Files encrypted post attack with ".C3680868C" extension.

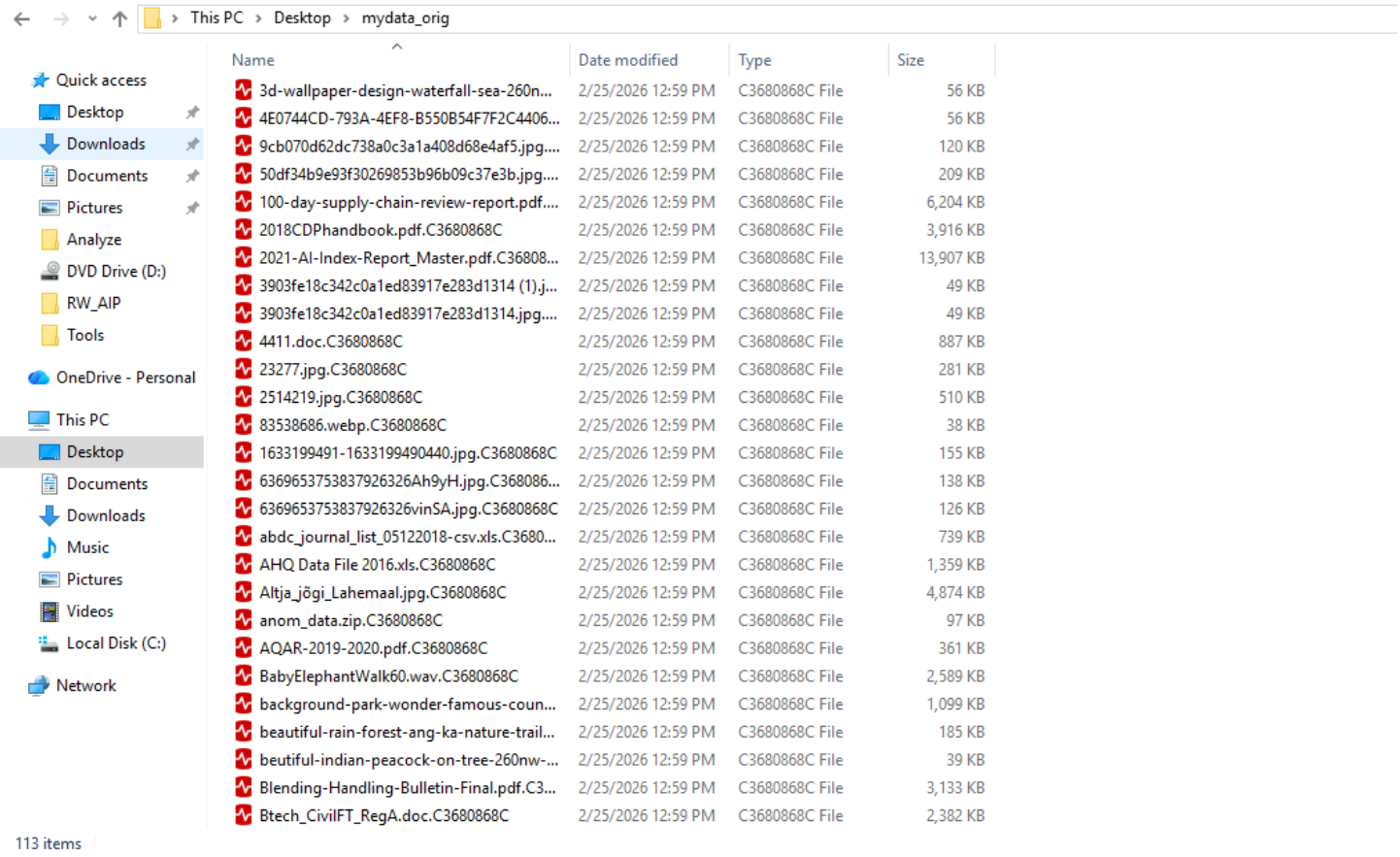
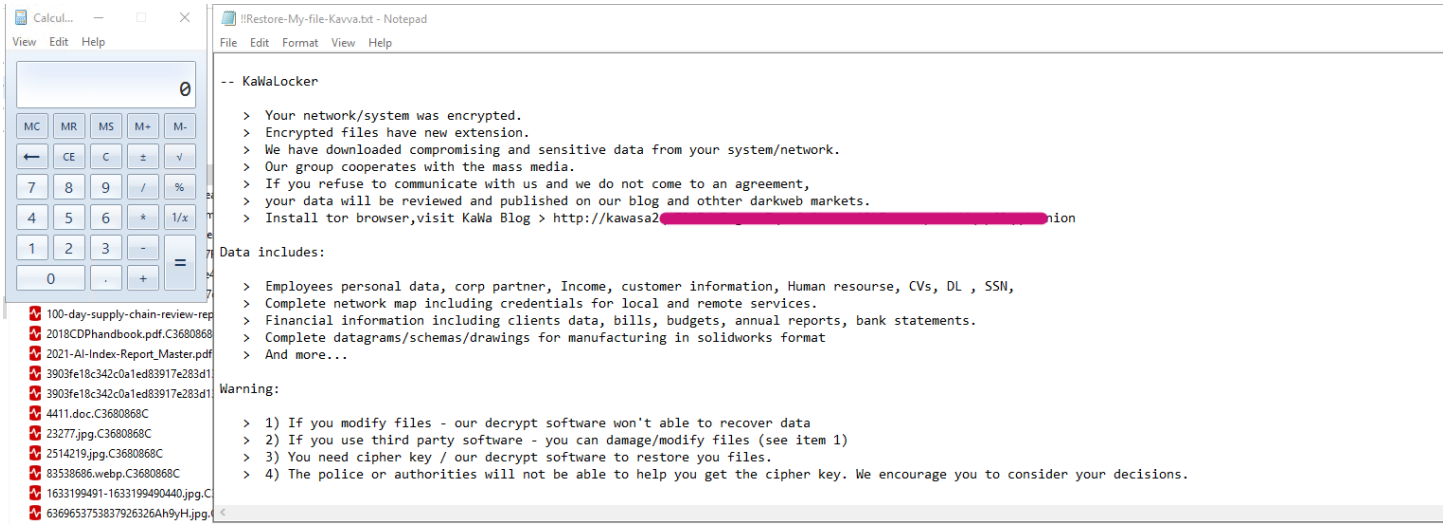
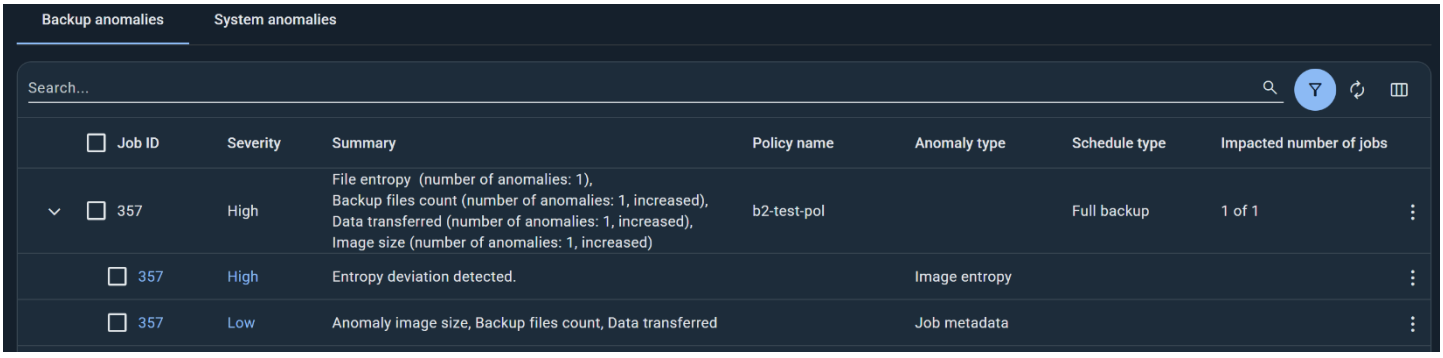


Image: Ransom Note named "!!Restore-My-file-Kavva.txt" dropped along with recovery details.



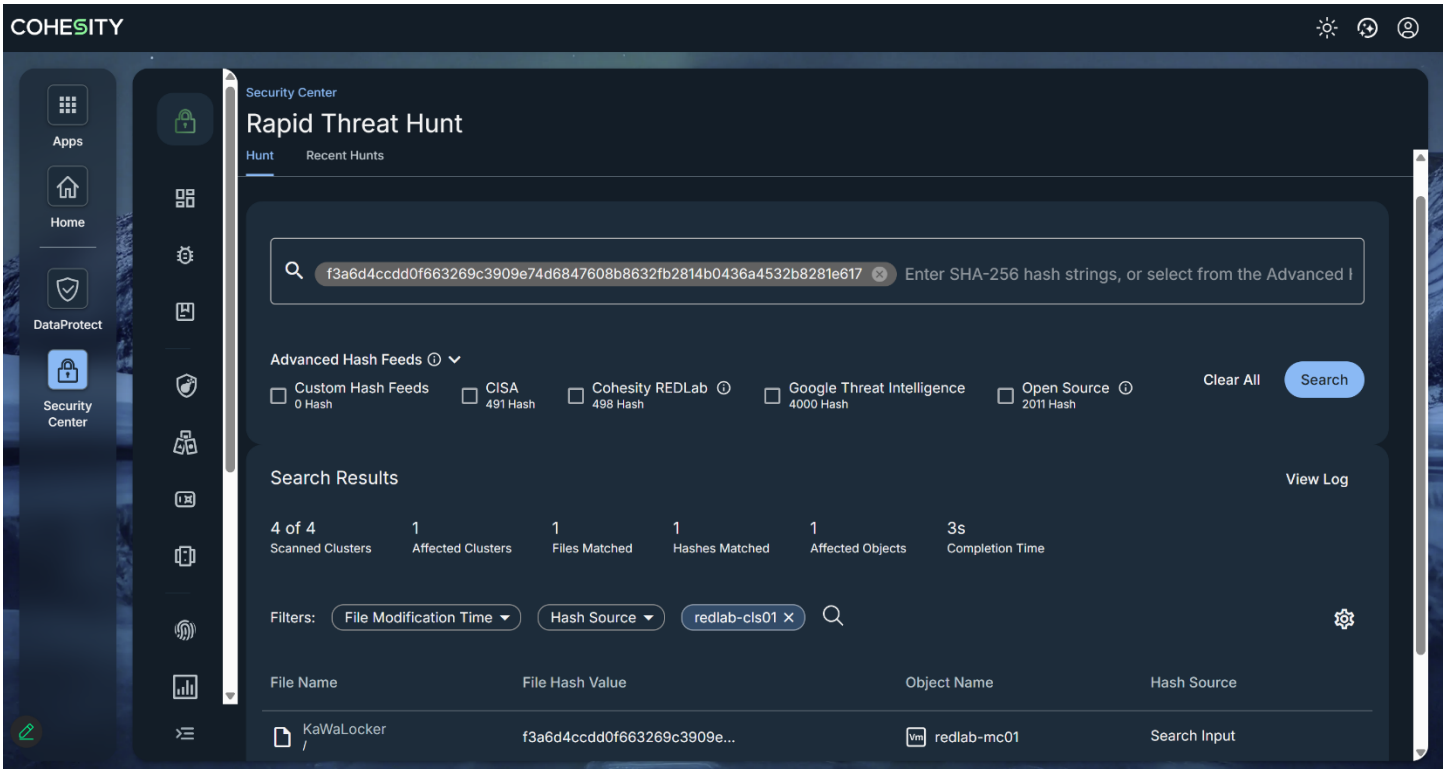
Protection & Detection Outcomes

After the attack, the DataProtect Agent backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.



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 KaWaLocker ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.



This capability enables security teams to quickly pivot from detection to investigation, validate threat presence, and assess potential blast radius across protected workloads.

Lockis Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Modify Registry	T1112	Persistence, Defense Evasion
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Registry Run Keys / Startup Folder	T1547.001	Persistence, Privilege Escalation
Abuse Elevation Control Mechanism	T1548	Privilege Escalation, Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal on Host	T1070	Defense Evasion
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Data Encrypted for Impact	T1486	Impact
Data Destruction	T1485	Impact

Malware impact post execution

Lockis ransomware is a crypto-ransomware strain that typically gains initial access through phishing payloads or exposed services, then establishes persistence and begins system reconnaissance. During examination, we found that Lockis encrypts files using strong cryptographic routines and appends the **“.lockis”** extension to affected data, making it inaccessible. It also creates a ransom note file named **“how_to_back_files.html”** containing payment instructions. Additionally, it may delete Volume Shadow Copies and terminate security processes to hinder recovery efforts and maximize impact.

Image: Files encrypted post attack with “.lockis” extension.

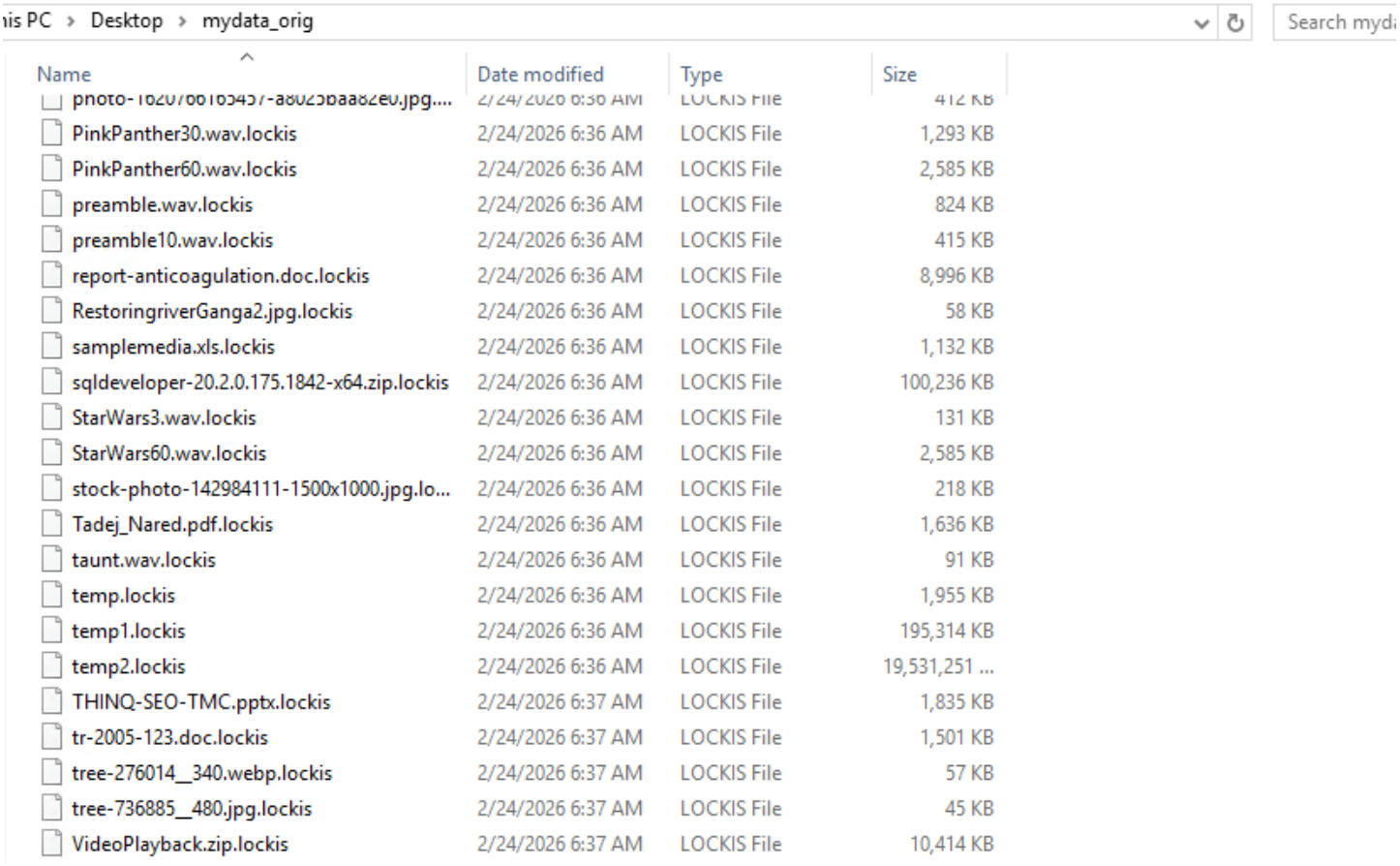
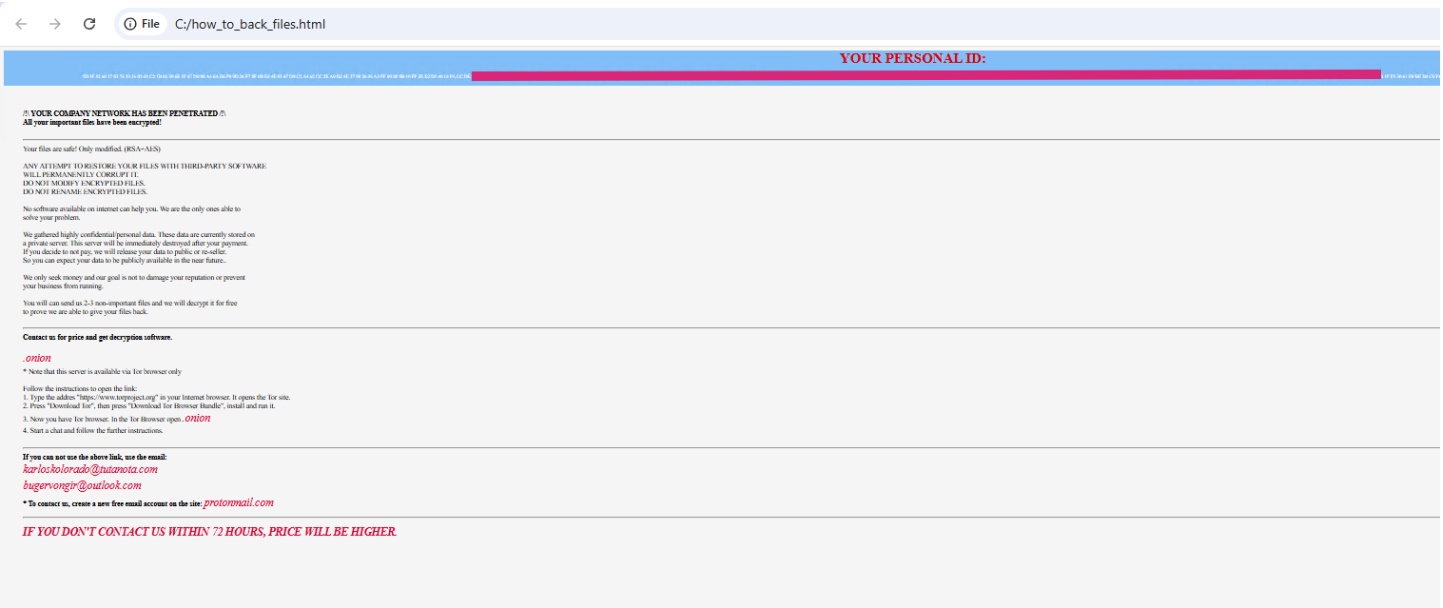
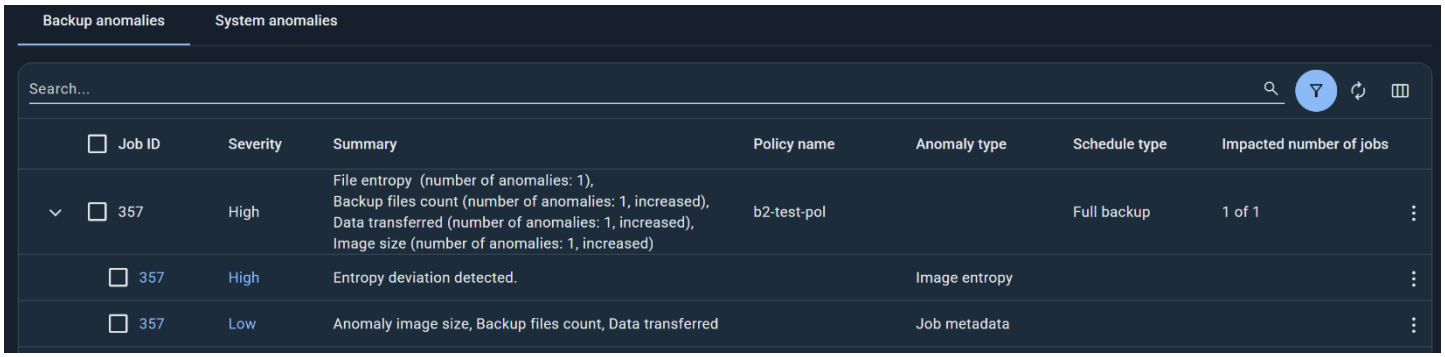


Image: Ransom Note named "how_to_back_files.html" dropped along with recovery details.



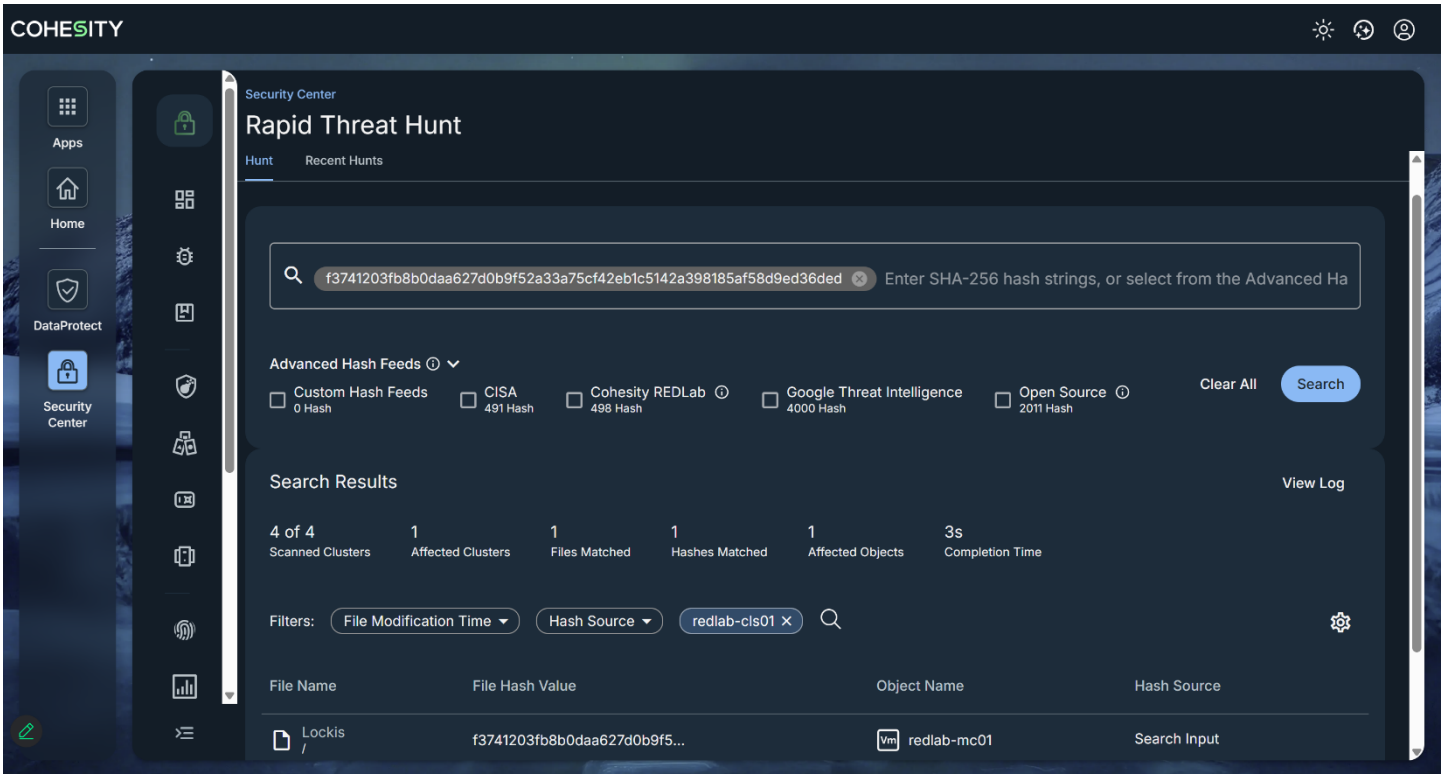
Protection & Detection Outcomes

After the attack, the DataProtect Agent backup operations remained unaffected. Despite the ransomware attack backups were executed successfully. Also, in the case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.



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 Lockis ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.



This capability enables security teams to quickly pivot from detection to investigation, validate threat presence, and assess potential blast radius across protected workloads.

Summary

- For all the ransomware strains described earlier, protection runs for the DataProtect Agent remained unaffected. Despite the ransomware attack, backups were executed successfully, demonstrating the platform's resilience and ability to maintain data protection under adverse conditions and recovery was validated as successful.

- In case of NetBackup Client a Job Metadata anomaly that detected unusual deviation in backup job attributes was generated. Along with it, due to changes in file attributes, an Image Entropy Data anomaly was also generated.

- 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