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: Sarcoma Family: Sarcoma Ransomware Group	6669cfeba5619b6f4d80b1281adfe69c87d845ebaaf9e83c25efa01a8267e751
Name: Novalock Family: GlobeImposter Ransomware Family	a2c7b8f2e8f560f309789ae882526973dcea5f0f693063b351179a14a20ef636
Name: SilentAnonymous Family: HiddenTear Ransomware Family	96fcbc8fde12e9db3c1786f71895a77f59d8c42cc9598c435bd73eb82f057087
Name: Handala Family: Handala Hack Group	fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2

Sarcoma Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Windows Management Instrumentation	T1047	Execution
Scheduled Task/Job	T1053	Execution, Persistence, Privilege Escalation
Command and Scripting Interpreter	T1059	Execution
Scripting	T1064	Execution, Defense Evasion
PowerShell	T1086	Execution
Native API	T1106	Execution
Process Injection	T1055	Privilege Escalation, Defense Evasion
Access Token Manipulation	T1134	Privilege Escalation, Defense Evasion
Abuse Elevation Control Mechanism	T1548	Privilege Escalation, Defense Evasion
Direct Volume Access	T1006	Defense Evasion
Rootkit	T1014	Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Software Packing	T1045	Defense Evasion
Indicator Removal	T1070	Defense Evasion
OS Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
Data Encrypted for Impact	T1486	Impact
Resource Hijacking	T1496	Impact

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

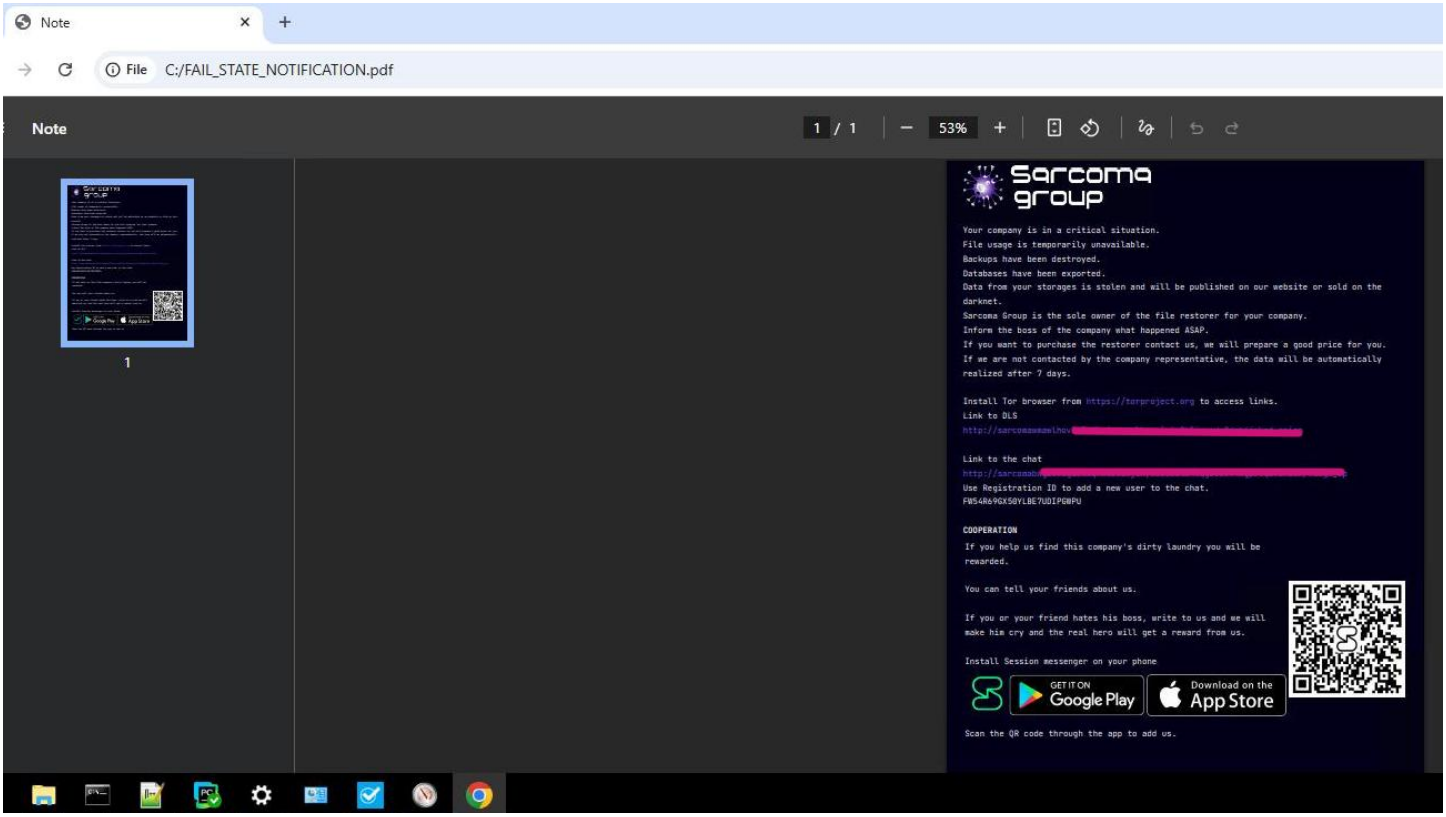
Malware impact post execution

Sarcoma ransomware is a double-extortion ransomware strain first observed in late 2024. Post execution, Sarcoma encrypts user and system files on both local and network-accessible drives using strong hybrid encryption algorithms, such as ChaCha20 combined with RSA. Encrypted files are renamed with a randomized extension such as ".xp9Mq1ZD05", which may vary per campaign. The malware drops a ransom note named "FAIL_STATE_NOTIFICATION.pdf", claiming data theft and threatening public disclosure via a leak site if ransom demands are not met. Sarcoma primarily targets Windows environments and is commonly associated with phishing, exploitation of public-facing applications and abuse of valid credentials for initial access.

Image: Files encrypted post attack with ".xp9Mq1ZD05" extension.

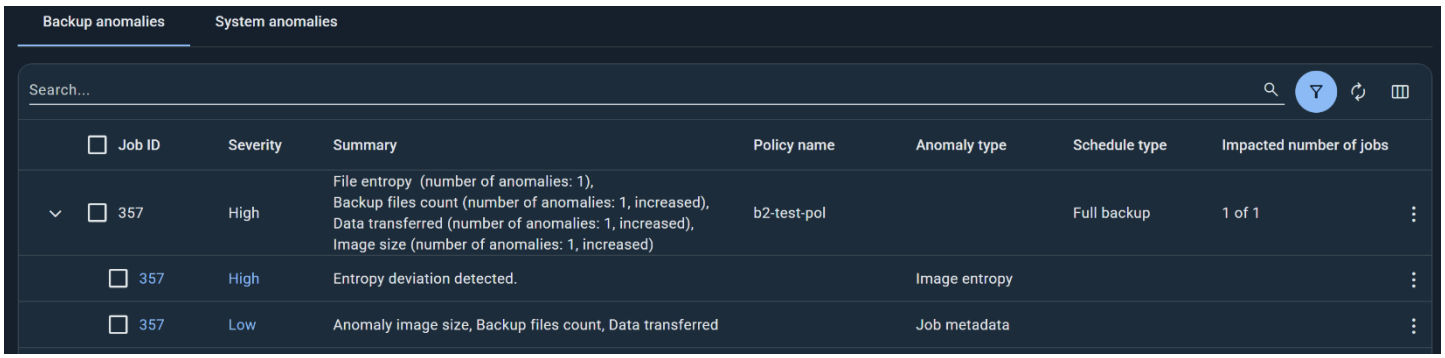
Name	Date modified	Type	Size
4411.doc.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	886 KB
23277.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	280 KB
2514219.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	509 KB
83538686.webp.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	37 KB
1633199491-1633199490440.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	154 KB
6369653753837926326Ah9yH.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	137 KB
6369653753837926326vinSA.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	125 KB
abdc_journal_list_05122018-csv.xls.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	738 KB
AHQ Data File 2016.xls.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	1,358 KB
Altja_jõgi_Lahemaal.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	4,873 KB
anom_data.zip.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	96 KB
AQAR-2019-2020.pdf.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	360 KB
BabyElephantWalk60.wav.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	2,588 KB
background-park-wonder-famous-countryside-waterscape_1417-1105.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	1,098 KB
beautiful-rain-forest-ang-ka-nature-trail-doi-inthanon-national-park-thailand-36703721.jpg.xp9Mq1...	3/18/2026 11:39 AM	XP9MQ1ZD05 File	184 KB
beutiful-indian-peacock-on-tree-260nw-2031028856.webp.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	38 KB
Blending-Handling-Bulletin-Final.pdf.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	3,132 KB
Btech_CivilFT_RegA.doc.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	2,381 KB
c4d5c1db2688b9da8dd1a9fd22bd17d2.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	119 KB
CantinaBand3.wav.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	133 KB
CantinaBand60.wav.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	2,588 KB
ClassAutoSearchTraffic.pdf.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	484 KB
CSE-2018_04_24.doc.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	2,435 KB
CV-Europass-A.M-29.09.2021.doc.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	276 KB
Cyber-Handbook-Enterprise.pdf.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	8,919 KB
download.jpg.xp9Mq1ZD05	3/18/2026 11:39 AM	XP9MQ1ZD05 File	11 KB

Image: Ransom Note named "FAIL_STATE_NOTIFICATION.pdf" dropped along with recovery details.



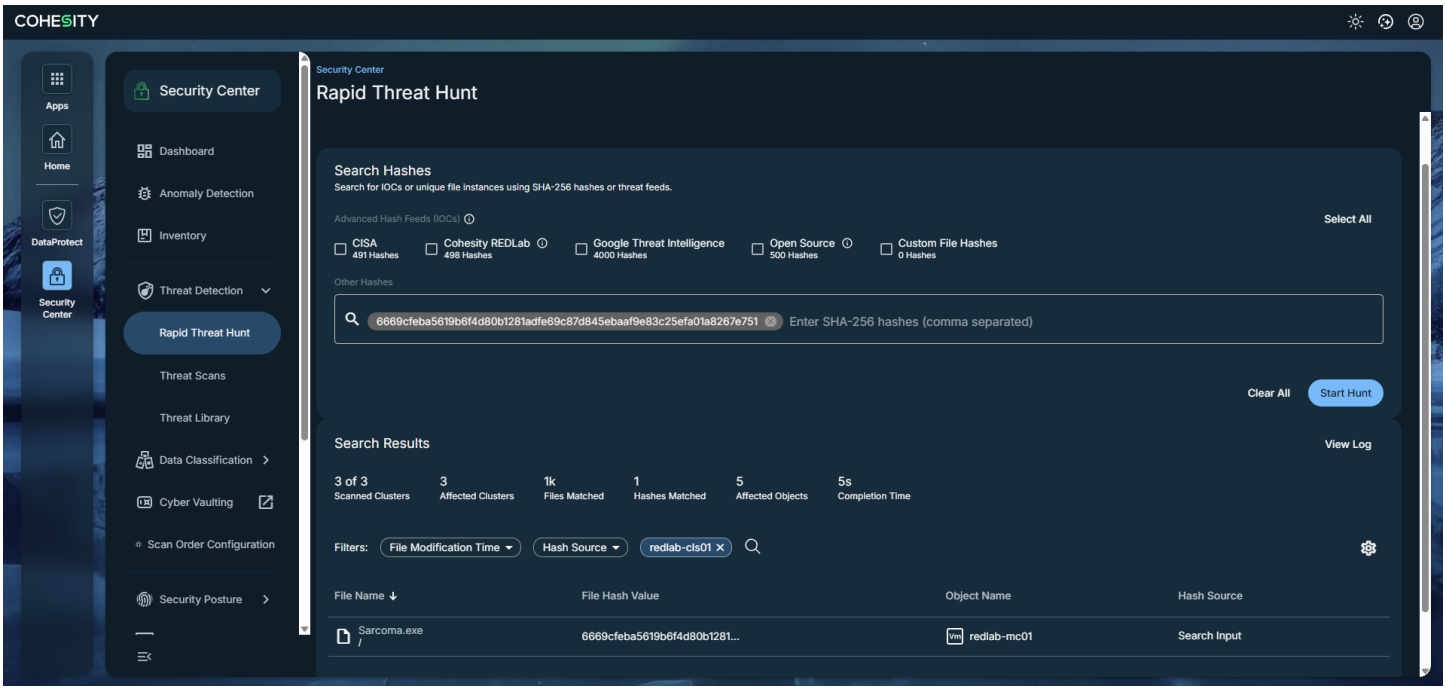
Protection & Detection Outcomes

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 Sarcoma 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.

Novalock Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
OS Credential Dumping	T1003	Credential Access
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Shared Modules	T1129	Execution
Modify Registry	T1112	Persistence, Defense Evasion
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Hijack Execution Flow	T1574	Persistence, Privilege Escalation, Defense Evasion
Abuse Elevation Control Mechanism	T1548	Privilege Escalation, Defense Evasion
Indicator Removal	T1070	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
Input Capture	T1056	Credential Access, Collection
Data from Local System	T1005	Collection
Email Collection	T1114	Collection
Query Registry	T1012	Discovery

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

Malware impact post execution

Novalock ransomware is a file-encrypting ransomware strain belonging to the GlobeImposter ransomware family. Post execution, Novalock encrypts user and system files on local and network-accessible drives using strong cryptographic algorithms, AES combined with RSA and appends the ".novalock" extension to affected files. Once encryption is complete, the malware drops a ransom note titled "how_to_back_files.html", stating that the victim's corporate network has been breached, files have been encrypted and sensitive data has been exfiltrated. The ransom note warns against using third-party recovery tools and threatens public disclosure of stolen data if ransom demands are not met. Novalock primarily targets Windows environments and is commonly associated with phishing emails, malicious attachments and compromised credentials, with a clear focus on business and corporate networks rather than individual users.

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

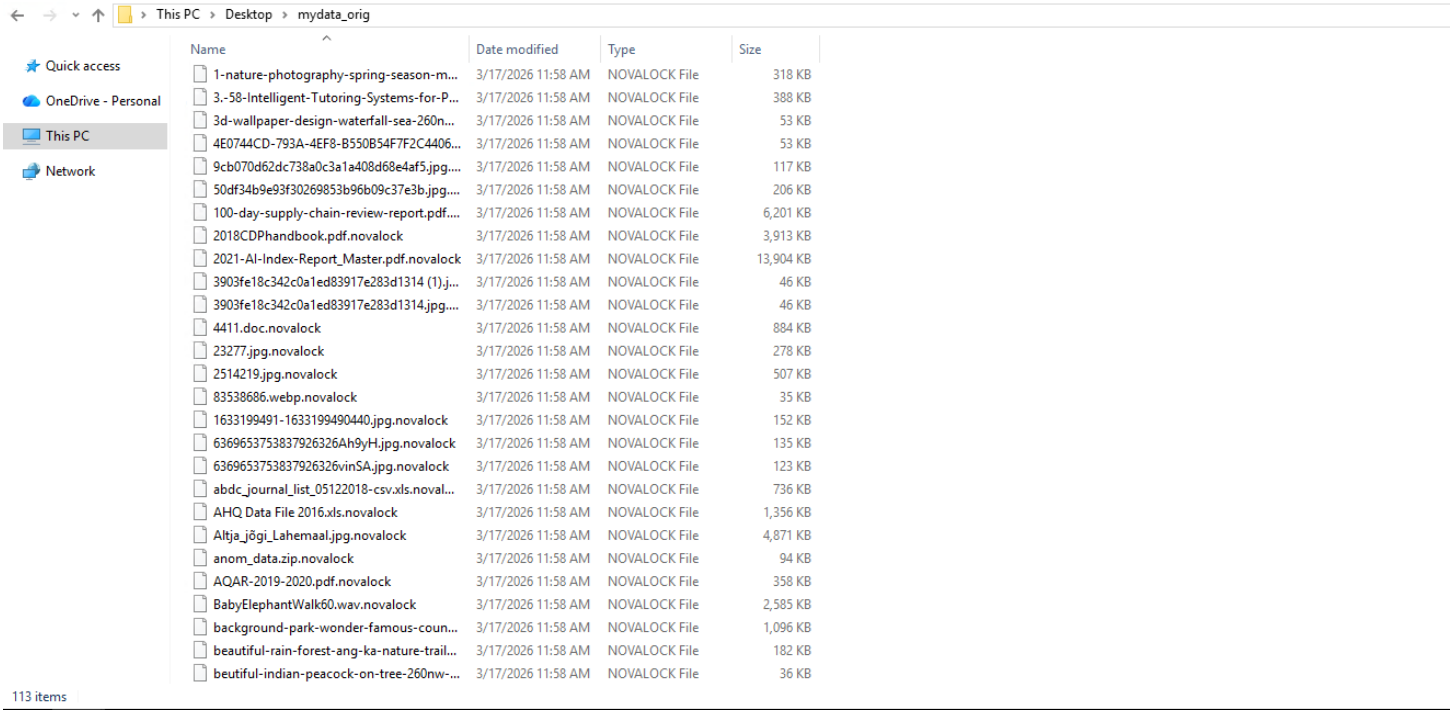
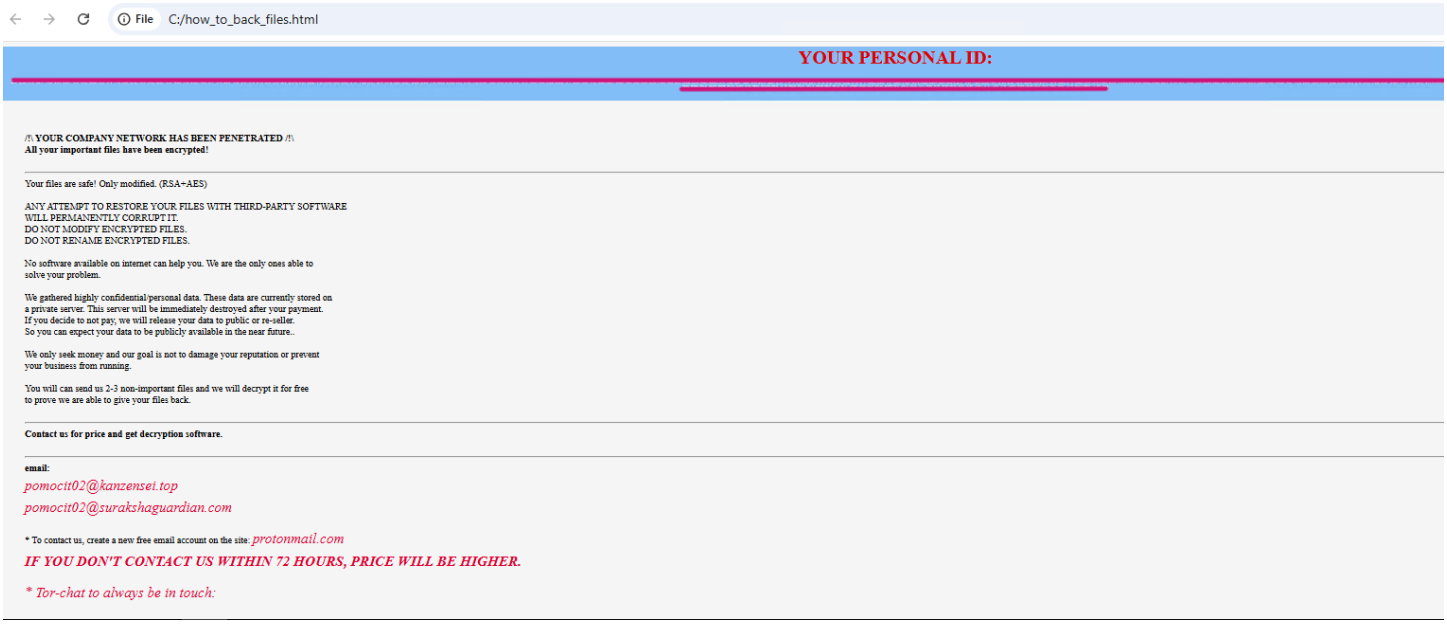
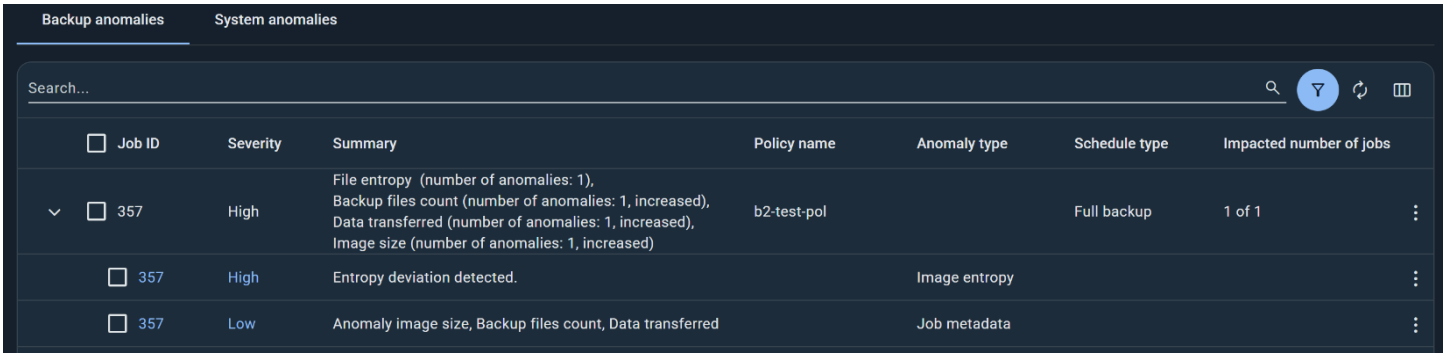


Image: Ransom Note named "how_to_back_files.html" dropped along with recovery details.



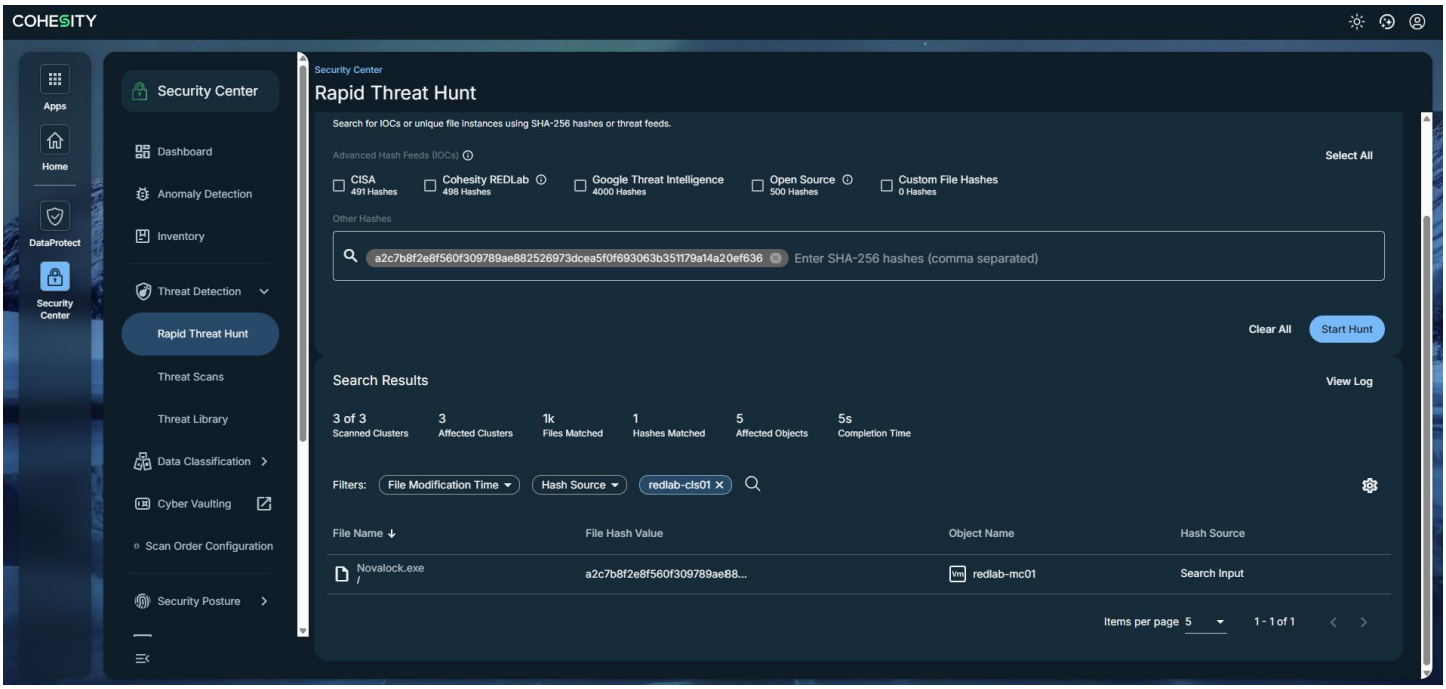
Protection & Detection Outcomes

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 Novalock 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.

SilentAnonymous Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Deobfuscate/Decode Files or Information	T1140	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
Virtualization / Sandbox Evasion	T1497	Defense Evasion; Discovery
Impair Defenses	T1562	Defense Evasion
OS Credential Dumping	T1003	Credential Access
Application Window Discovery	T1010	Discovery
Query Registry	T1012	Discovery
System Owner/User Discovery	T1033	Discovery
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Account Discovery	T1087	Discovery
Software Discovery	T1518	Discovery
Data from Local System	T1005	Collection
Clipboard Data	T1115	Collection
Browser Session Hijacking	T1185	Collection

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

Malware impact post execution

SilentAnonymous ransomware is a Windows-targeting ransomware strain associated with the HiddenTear ransomware family. Post execution, SilentAnonymous encrypts user and system files with AES-based encryption and appends the ".SILENTATTACK" extension to affected files. Following encryption, the malware drops a ransom note named "Silent_Anon.txt", informing victims that their data has been encrypted and demanding payment for recovery. SilentAnonymous establishes persistence and performs extensive system, file and account discovery prior to encryption, enabling broad coverage across the compromised environment.

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

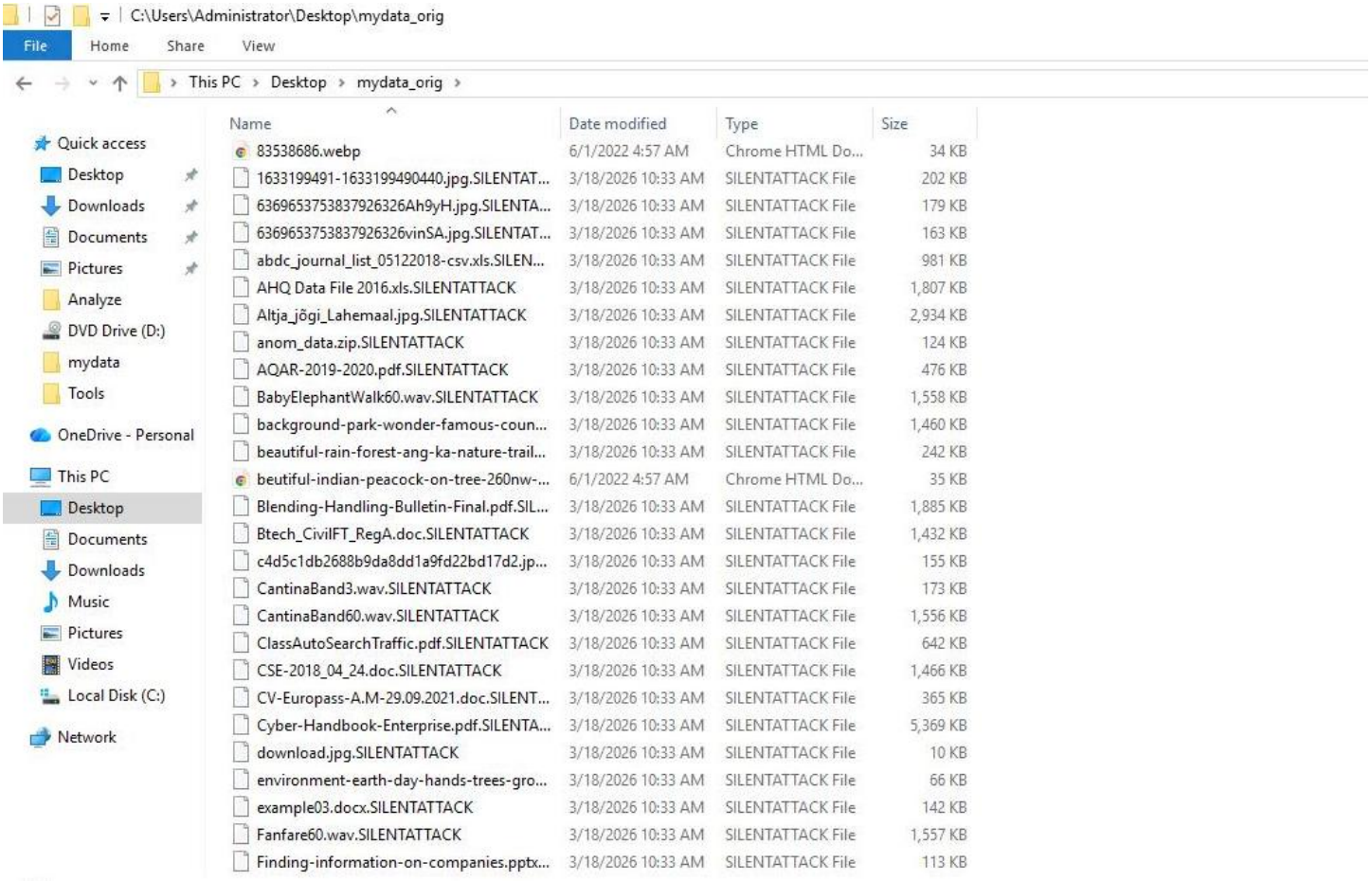
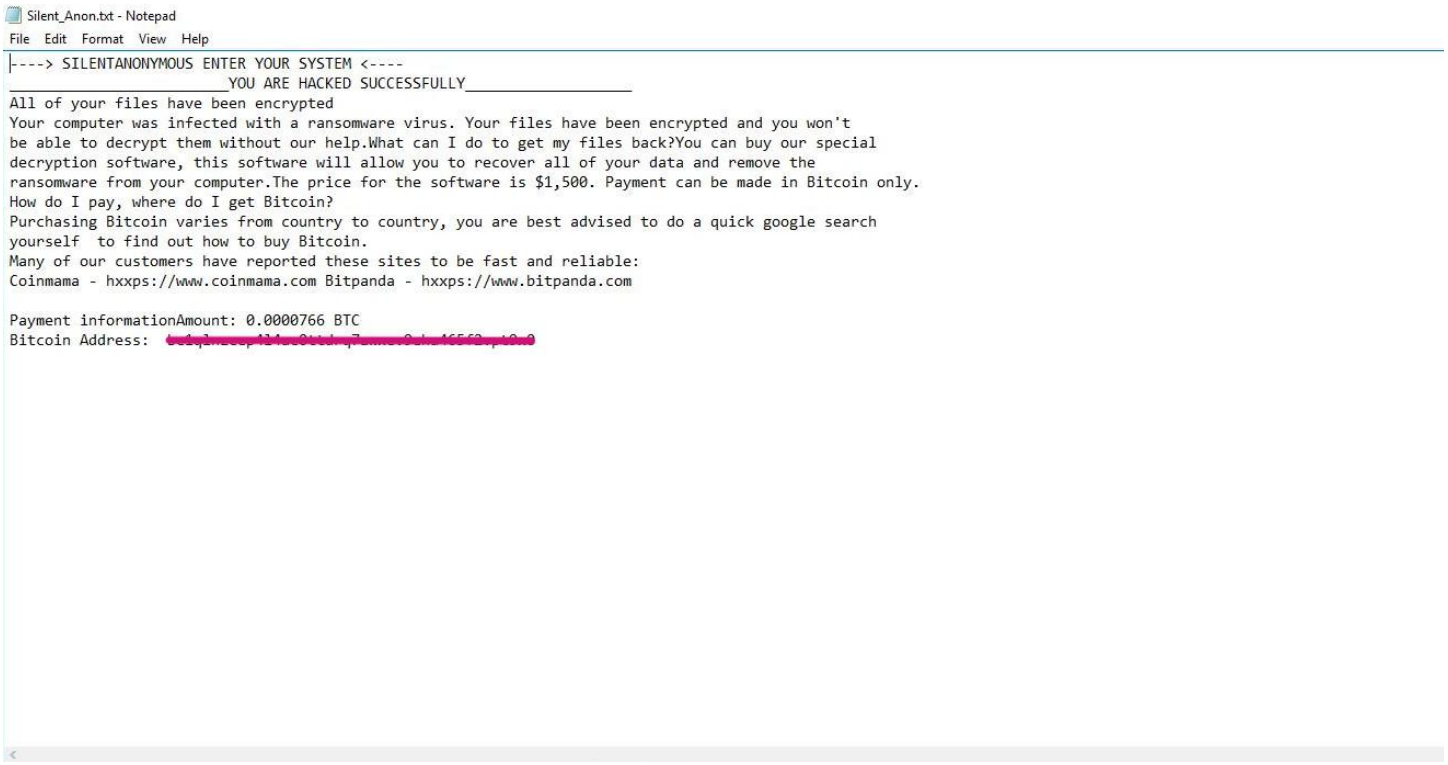
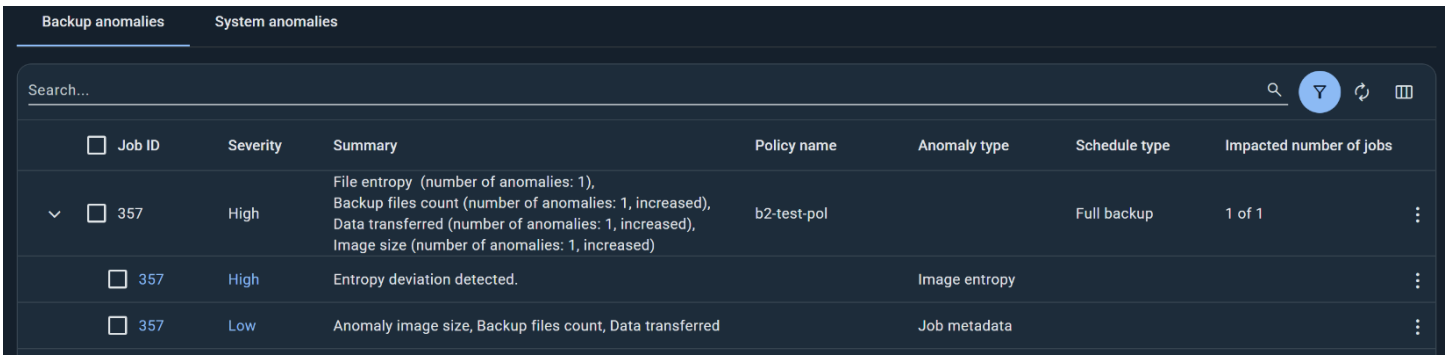


Image: Ransom Note named "Silent_Anon.txt" dropped along with recovery details.



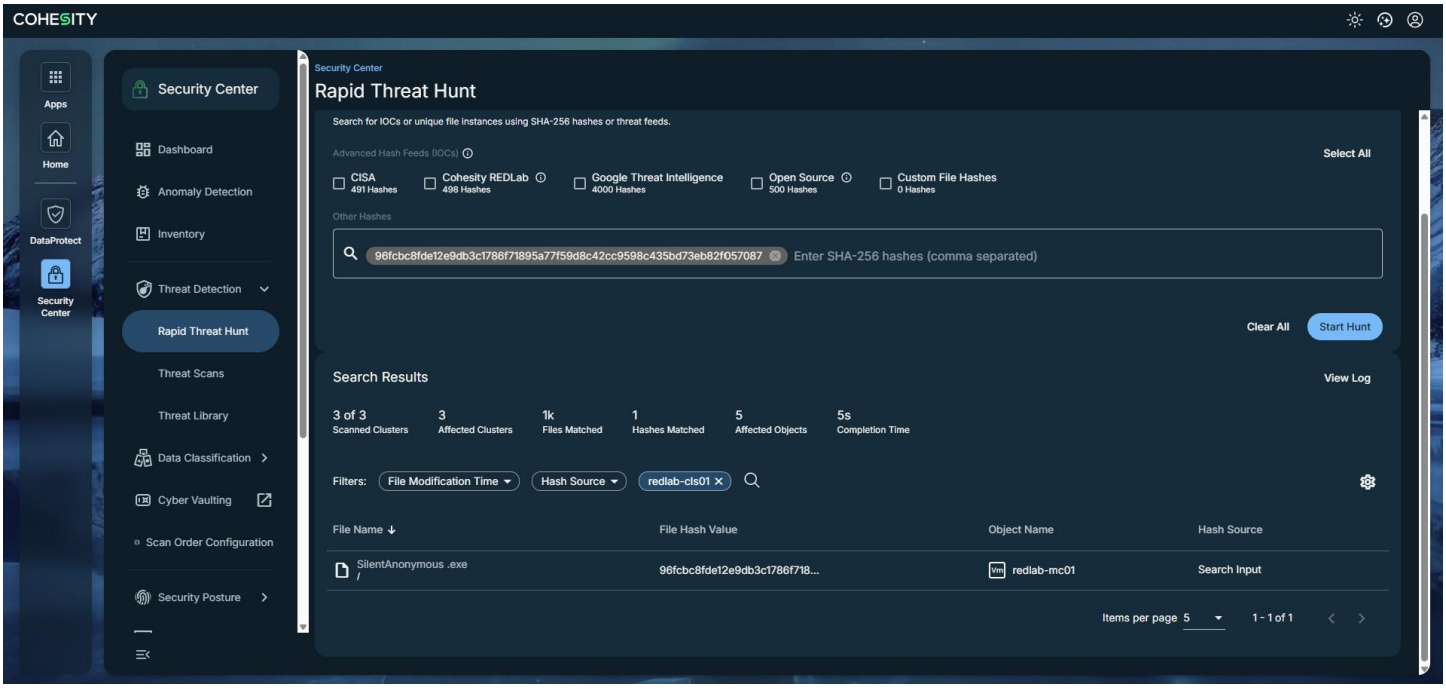
Protection & Detection Outcomes

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 SilentAnonymous 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.

Handala Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Native API	T1106	Execution
Shared Modules	T1129	Execution
SIP and Trust Provider Hijacking	T1198	Persistence; Defense Evasion
Process Injection	T1055	Privilege Escalation; Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Impair Defenses	T1562	Defense Evasion
Input Capture	T1056	Credential Access; Collection
System Network Configuration	T1016	Discovery
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery

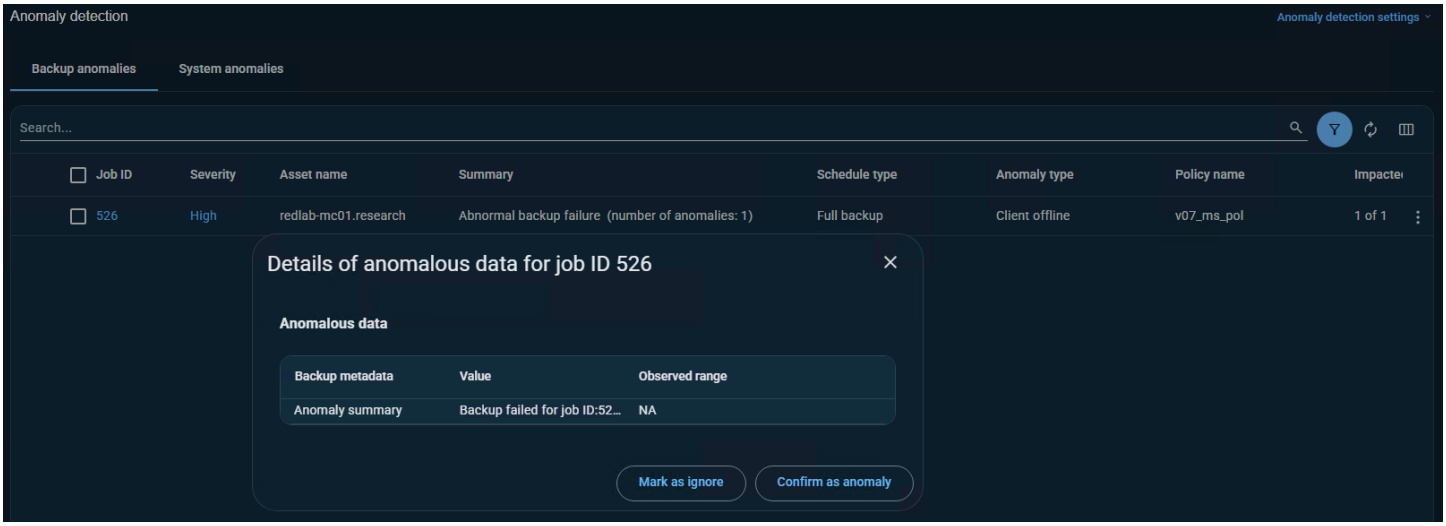
Note: Above table contains a curated subset of techniques prioritized for monitoring and response.*

Malware impact post execution

Handala ransomware is a destructive wiper-type ransomware associated with the Handala Hack Group, first observed in December 2023. The group has been active in recent campaigns, including large-scale destructive attacks observed in March 2026 targeting major enterprise and critical infrastructure organizations. Unlike traditional ransomware, Handala does not encrypt files but post execution, it permanently deletes user and system files across local and network-accessible drives, resulting in irreversible data loss. As the malware performs data destruction rather than encryption, no cryptographic algorithm is used and no ransomware-specific file extension is appended to affected files. Handala leverages native API execution, process injection, system and file discovery and multiple defense-evasion techniques to impair security controls prior to data deletion. The malware is commonly associated with phishing-based initial access and manual attacker-driven execution, with the primary objective being operational disruption rather than financial extortion.

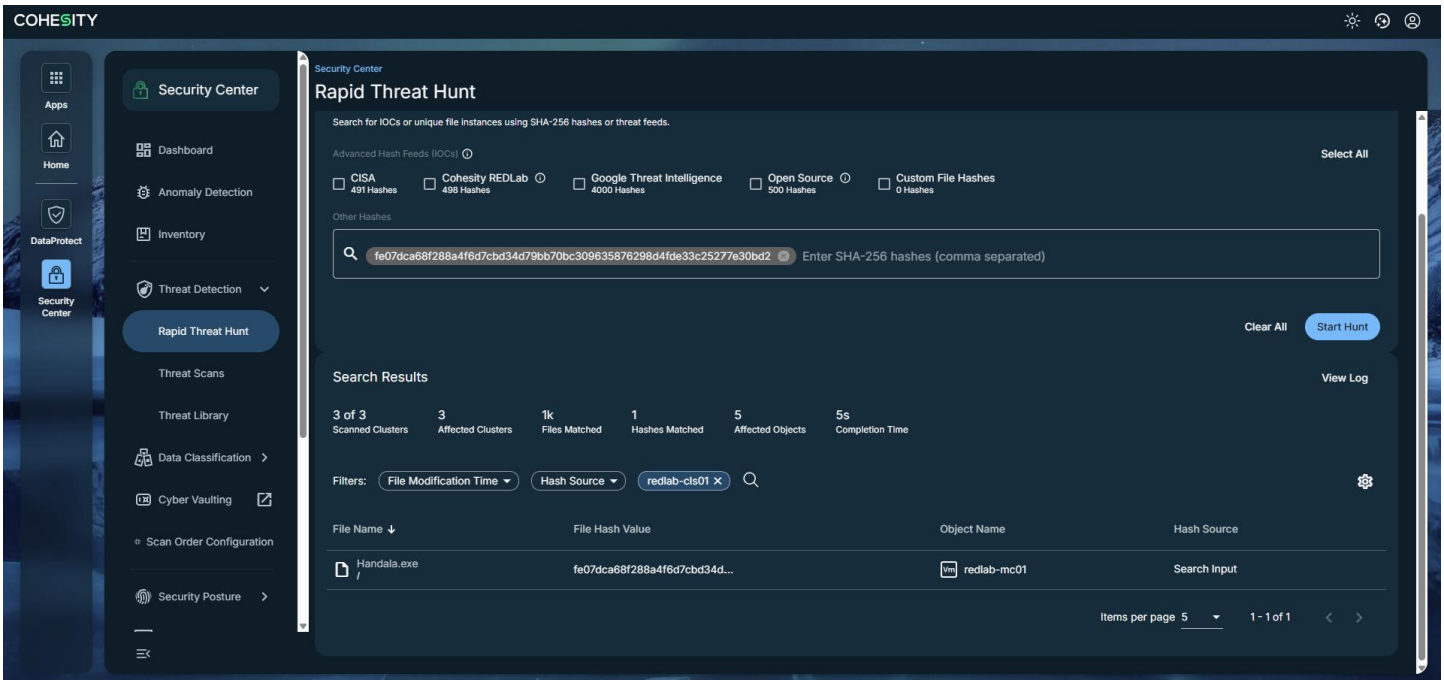
Protection & Detection Outcomes

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 data on victim machine (Client) is encrypted along with NetBackup configuration files and a backup anomaly that detects unusual behavior with respect to offline clients was 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 Handala 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 for Sarcoma, Novalock and SilentAnonymous.

- While in case of Handala ransomware strain data on NetBackup client is encrypted along with NetBackup configuration files and a backup anomaly that detects unusual behavior with respect to offline clients was 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