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: VanHelsing Family: VanHelsing Ransomware Group	86d812544f8e250f1b52a4372aaab87565928d364471d115d669a8cc7ec50e17
Name: Find Family: Dharma Ransomware Family	5d615b405ab601e187be494805227e7dc96316ef06813eaa4b9c10ac93d1fd56
Name: Trial_recovery Family: Trigona Ransomware Family	b0dfaf509de38749c49afcb3cd34d27126044bb77cc16896b02ebced6f95db02
Name: Payload Family: Payload Ransomware Group	1ca67af90400ee6cbbd42175293274a0f5dc05315096cb2e214e4bfe12ffb71f

VanHelsing 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
Shared Modules	T1129	Execution
Hijack Execution Flow	T1574	Execution, Stealth
Modify Registry	T1112	Persistence, Defense Impairment
Pre-OS Boot	T1542	Persistence, Stealth
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Process Injection	T1055	Privilege Escalation, Stealth
Abuse Elevation Control Mechanism	T1548	Privilege Escalation
Direct Volume Access	T1006	Stealth
Rootkit	T1014	Stealth
Obfuscated Files or Information	T1027	Stealth
Masquerading	T1036	Stealth
Software Packing	T1045	Stealth
Indicator Removal	T1070	Stealth
File Deletion	T1107	Stealth
Hidden Window	T1143	Stealth

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

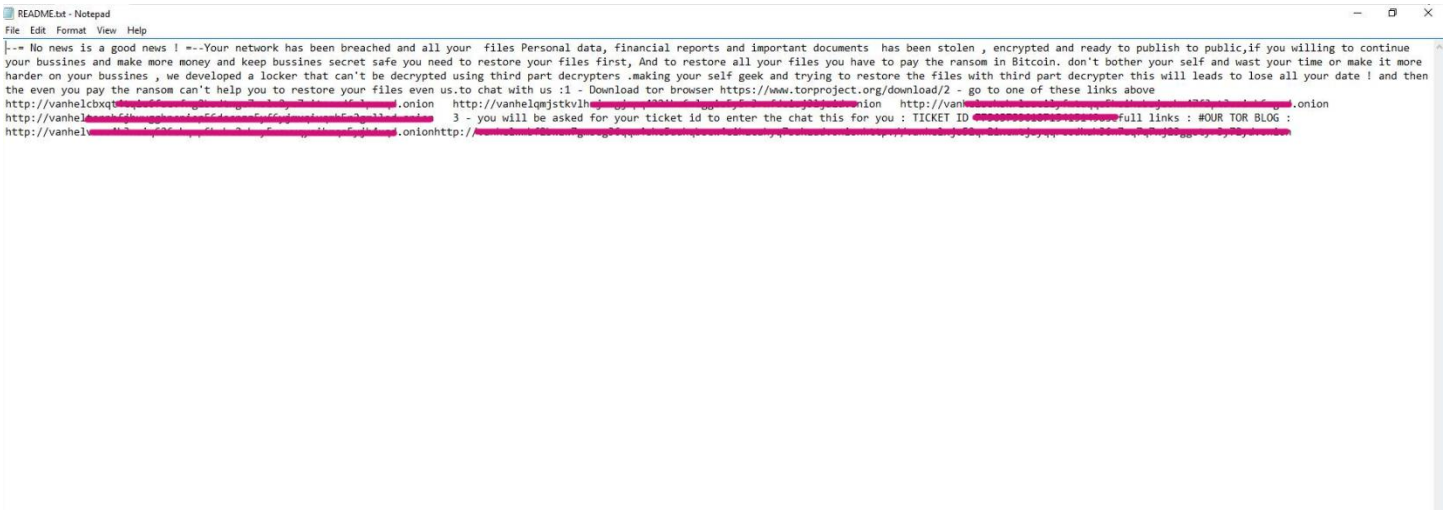
Malware impact post execution

VanHelsing ransomware is a Windows-targeting ransomware strain observed performing full-scale file encryption across compromised systems. Post execution, VanHelsing encrypts user and system files on both local and network-accessible drives using strong symmetric encryption and appends the“.vanhelsing” extension to affected files, rendering data inaccessible. Following encryption, the malware drops a ransom note named “README.txt”, instructing victims on recovery steps and ransom payment, indicating successful completion of the encryption phase.

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

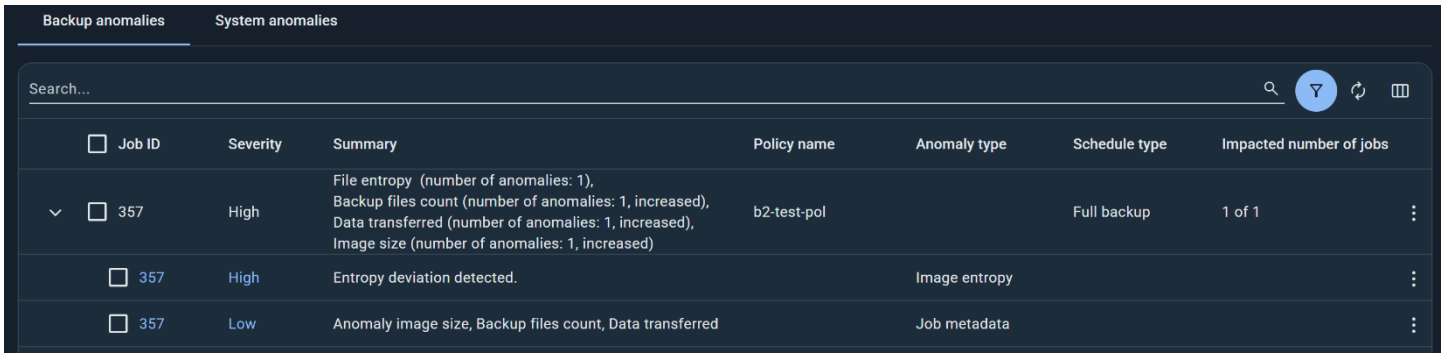
Name	Date modified	Type	Size
2021-AI-Index-Report_Master.pdf.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	13,904 KB
3903fe18c342c0a1ed83917e283d1314 (1).jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	45 KB
3903fe18c342c0a1ed83917e283d1314.jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	45 KB
4411.doc.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	883 KB
23277.jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	277 KB
2514219.jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	506 KB
83538686.webp.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	34 KB
1633199491-1633199490440.jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	152 KB
6369653753837926326Ah9yH.jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	134 KB
6369653753837926326vinSA.jpg.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	123 KB
abdc_journal_list_05122018-csv.xls.vanhelsing	4/20/2026 1:38 PM	VANHELSING File	736 KB
AHQ Data File 2016.xls.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	1,356 KB
Altja_jõgi_Lahemaal.jpg.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	4,871 KB
anom_data.zip.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	93 KB
AQAR-2019-2020.pdf.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	357 KB
BabyElephantWalk60.wav.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	2,585 KB
background-park-wonder-famous-countryside-waterscape_1417-1105.jpg.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	1,095 KB
beautiful-rain-forest-ang-ka-nature-trail-doi-inthanon-national-park-thailand-36703721.jpg.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	182 KB
beutiful-indian-peacock-on-tree-260nw-2031028856.webp.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	35 KB
Blending-Handling-Bulletin-Final.pdf.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	3,130 KB
Btech_CivilFT_RegA.doc.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	2,378 KB
c4d5c1db2688b9da8dd1a9fd22bd17d2.jpg.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	116 KB
CantinaBand3.wav.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	130 KB
CantinaBand60.wav.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	2,585 KB
ClassAutoSearchTraffic.pdf.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	482 KB
CSE-2018_04_24.doc.vanhelsing	4/20/2026 1:39 PM	VANHELSING File	2,433 KB

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



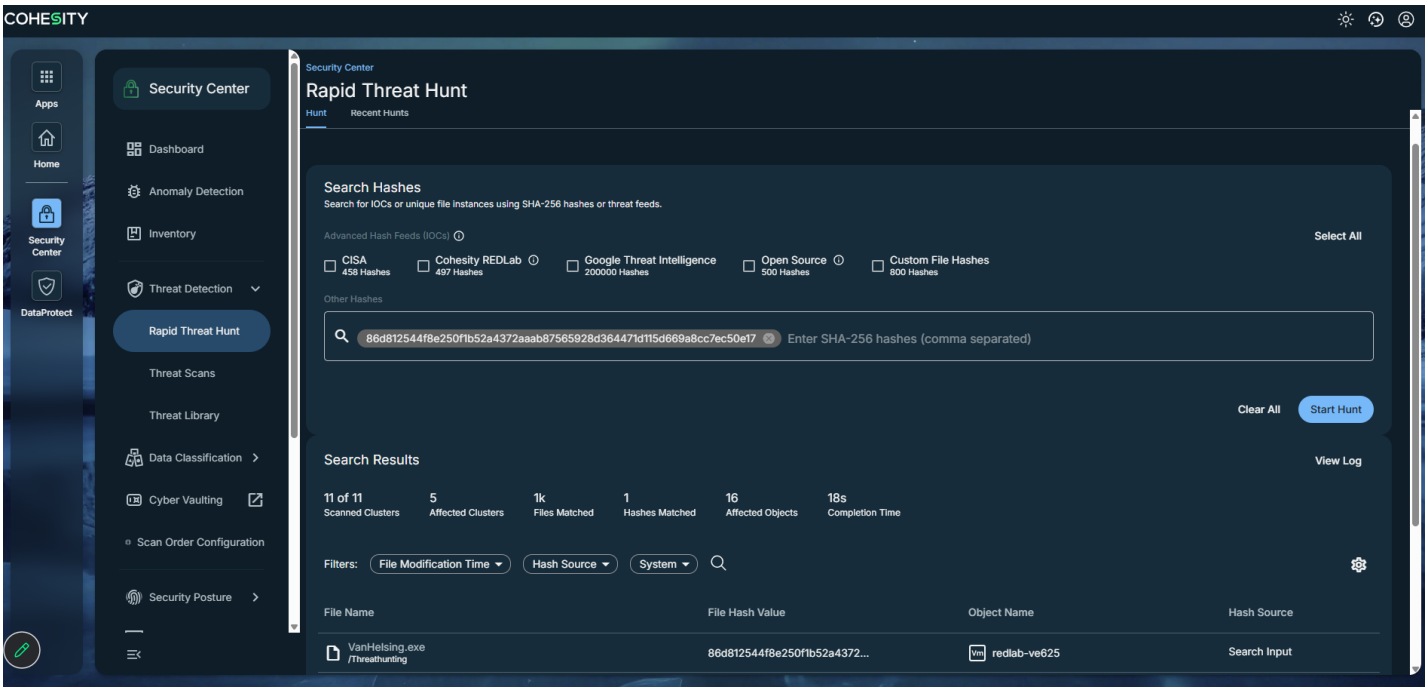
Protection & Detection Outcomes

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 VanHelsing 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.

Find Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Native API	T1106	Execution
Shared Modules	T1129	Execution
New Service	T1050	Persistence, Privilege Escalation
Registry Run Keys / Startup Folder	T1060	Persistence
Modify Registry	T1112	Persistence
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Access Token Manipulation	T1134	Privilege Escalation, Stealth
Obfuscated Files or Information	T1027	Stealth
Masquerading	T1036	Stealth
Software Packing	T1045	Stealth
Indicator Removal	T1070	Stealth
File Deletion	T1107	Stealth
Deobfuscate/Decode Files or Information	T1140	Stealth
Indirect Command Execution	T1202	Stealth
Virtualization/Sandbox Evasion	T1497	Stealth, Discovery
File and Directory Discovery	T1083	Discovery
System Location Discovery	T1614	Discovery
Data Staged	T1074	Collection

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

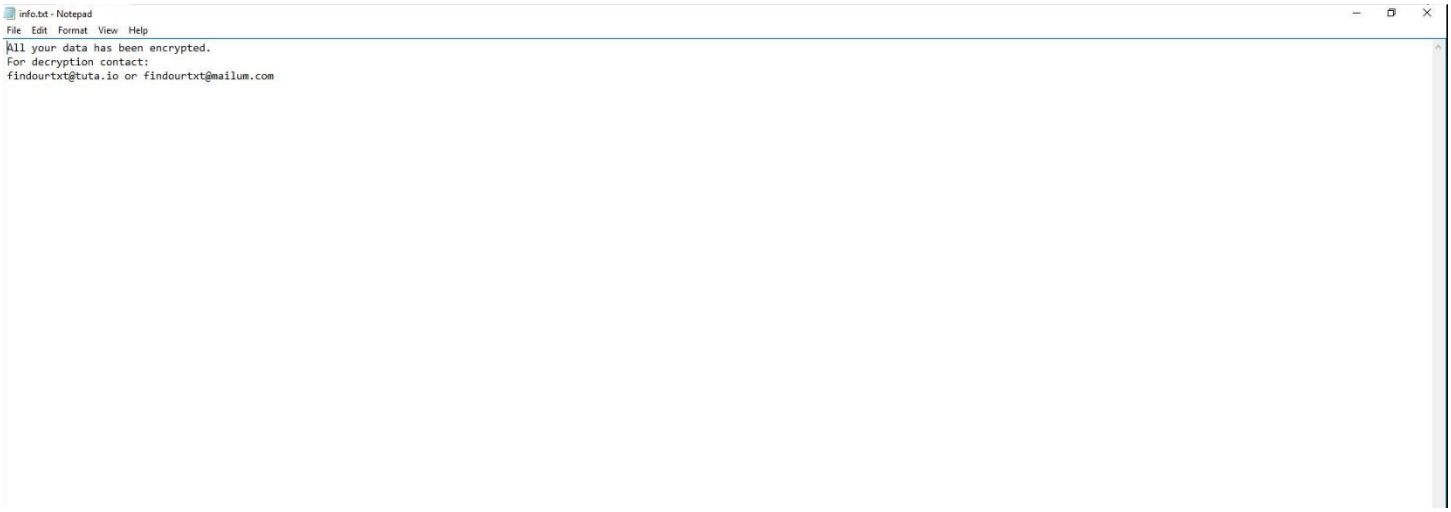
Malware impact post execution

Find ransomware, a variant of the Dharma (CrySiS) ransomware family, performs rapid file system enumeration and encrypts user and application data across local disks and network-accessible shares. Encrypted files are renamed to include a unique victim ID and attacker contact email, followed by the ".FIND" extension, rendering the data inaccessible and clearly marking affected assets. Find employs strong cryptographic routines consistent with the Dharma family, using AES-based symmetric encryption for file contents, with per-file keys protected using RSA public-key cryptography embedded within the ransomware binary. Post encryption, Find drops a ransom note named "info.txt" in affected directories and additionally displays a ransom notification to the user.

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

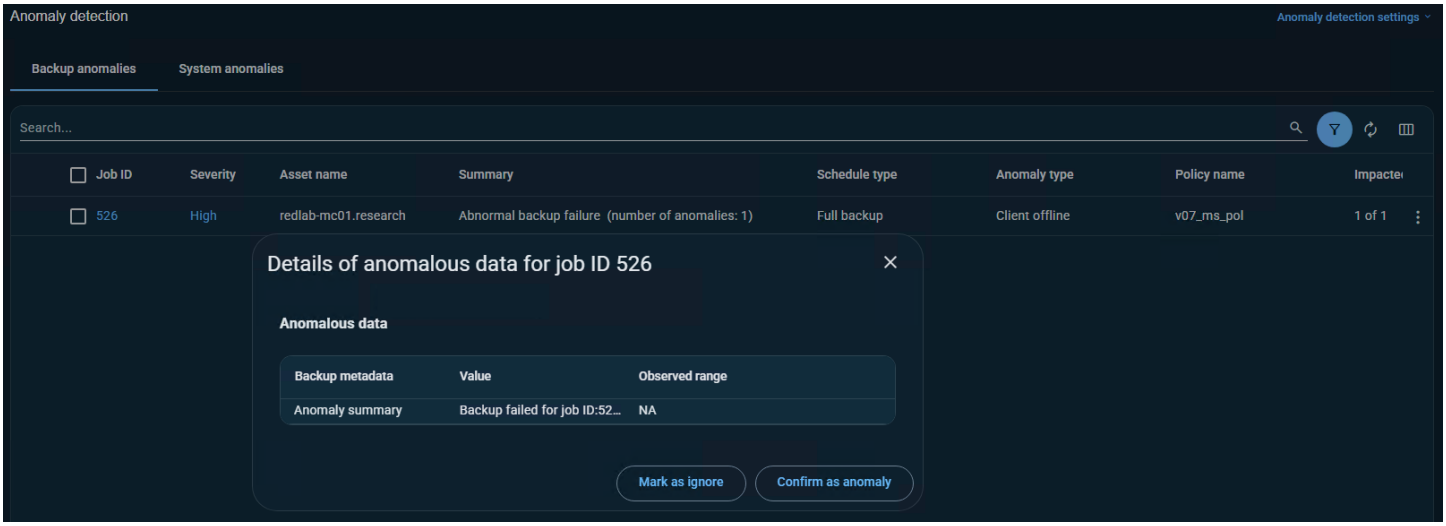
Name	Date modified	Type	Size
4411.doc.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	883 KB
23277.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:53 PM	FIND File	277 KB
2514219.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:53 PM	FIND File	506 KB
83538686.webp.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:53 PM	FIND File	34 KB
1633199491-1633199490440.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:53 PM	FIND File	151 KB
6369653753837926326Ah9yH.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:53 PM	FIND File	134 KB
6369653753837926326vinSA.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	123 KB
abdc_journal_list_05122018-csv.xls.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	736 KB
AHQ Data File 2016.xls.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	1,356 KB
Altja_jõgi_Lahemaal.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	5,639 KB
anom_data.zip.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	93 KB
AQAR-2019-2020.pdf.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	357 KB
BabyElephantWalk60.wav.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	3,353 KB
background-park-wonder-famous-countryside-waterscape_1417-1105.jpg.id-A0606706.[findourtxt@tuta.io].F...	4/22/2026 1:54 PM	FIND File	1,095 KB
beautiful-rain-forest-ang-ka-nature-trail-doi-inthanon-national-park-thailand-36703721.jpg.id-A0606706.[fin...	4/22/2026 1:54 PM	FIND File	182 KB
beutiful-indian-peacock-on-tree-260nw-2031028856.webp.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:53 PM	FIND File	35 KB
Blending-Handling-Bulletin-Final.pdf.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	3,897 KB
Btech_CivilFT_RegA.doc.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	3,146 KB
c4d5c1db2688b9da8dd1a9fd22bd17d2.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	116 KB
CantinaBand3.wav.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	130 KB
CantinaBand60.wav.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	3,353 KB
ClassAutoSearchTraffic.pdf.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	482 KB
CSE-2018_04_24.doc.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	3,201 KB
CV-Europass-A.M-29.09.2021.doc.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	274 KB
Cyber-Handbook-Enterprise.pdf.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	9,684 KB
download.jpg.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	8 KB
environment-earth-day-hands-trees-growing-seedlings-bokeh-green-background-female-hand-holding-tre...	4/22/2026 1:54 PM	FIND File	50 KB
example03.docx.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	107 KB
Fanfare60.wav.id-A0606706.[findourtxt@tuta.io].FIND	4/22/2026 1:54 PM	FIND File	3,353 KB

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



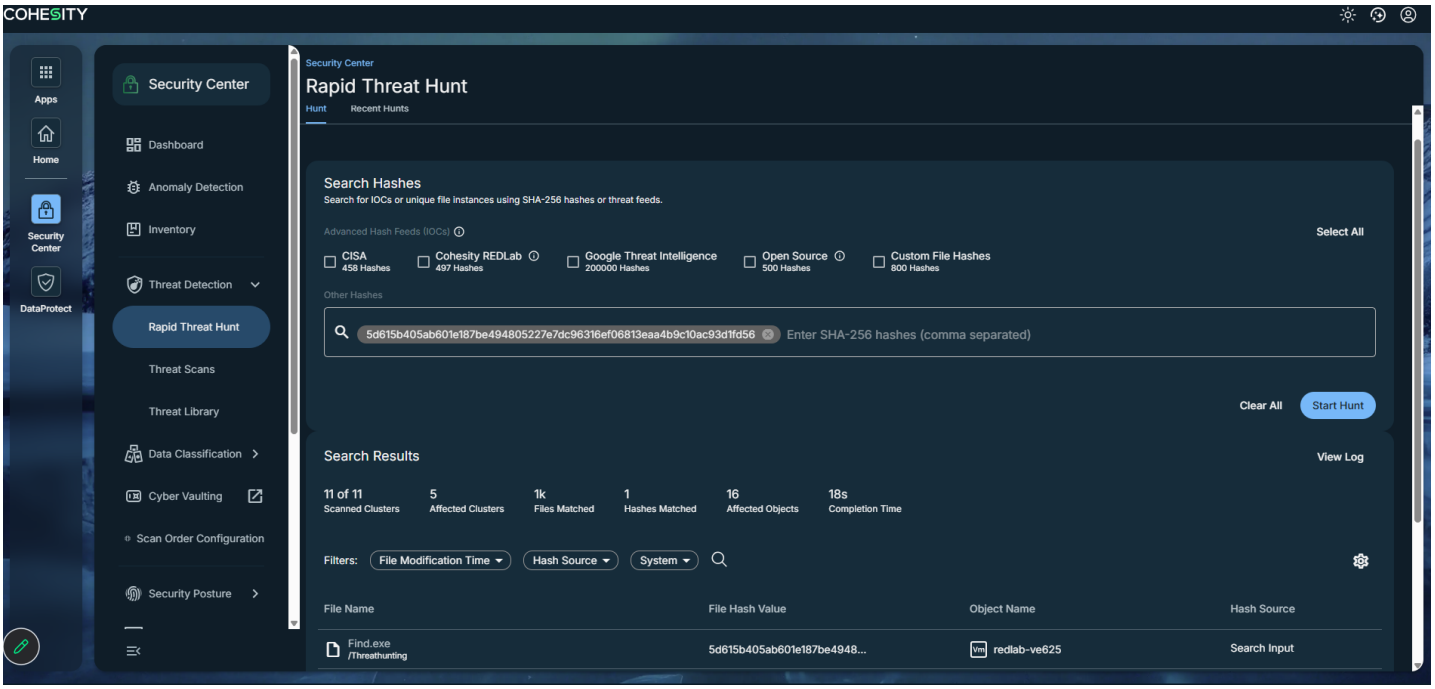
Protection & Detection Outcomes

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 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 Find 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.

Trial_recovery Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Native API	T1106	Execution
Shared Modules	T1129	Execution
Hijack Execution Flow	T1574	Execution, Stealth
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Process Injection	T1055	Privilege Escalation, Stealth
Obfuscated Files or Information	T1027	Stealth
Software Packing	T1045	Stealth
Indicator Removal	T1070	Stealth
File Deletion	T1107	Stealth
Hidden Window	T1143	Stealth
Indirect Command Execution	T1202	Stealth
Virtualization/Sandbox Evasion	T1497	Stealth, Discovery
Hide Artifacts	T1564	Stealth
Steal Web Session Cookie	T1539	Credential Access
System Service Discovery	T1007	Discovery
Application Window Discovery	T1010	Discovery
Query Registry	T1012	Discovery
Remote System Discovery	T1018	Discovery
Process Discovery	T1057	Discovery

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

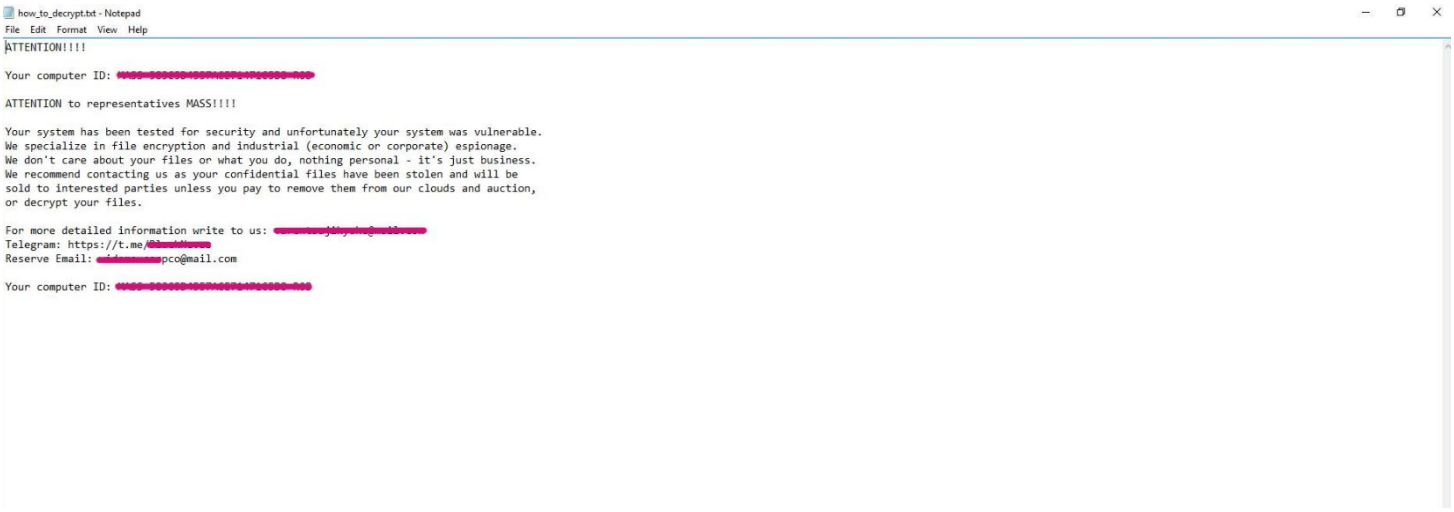
Malware impact post execution

Trial_recovery ransomware, a variant associated with the Trigona ransomware family, performs extensive file system enumeration and encrypts data across local drives, network-accessible shares, and mounted storage. Encrypted files are renamed using a distinctive pattern that prepends “trial-recovery”, appends randomized identifiers and adds the“.-encrypted” extension. Following encryption, Trial_recovery drops a ransom note named “how_to_decrypt.txt” in affected directories. The note informs victims that their files have been encrypted and claims that sensitive data has been exfiltrated, threatening to leak or sell stolen data if ransom demands are not met.

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

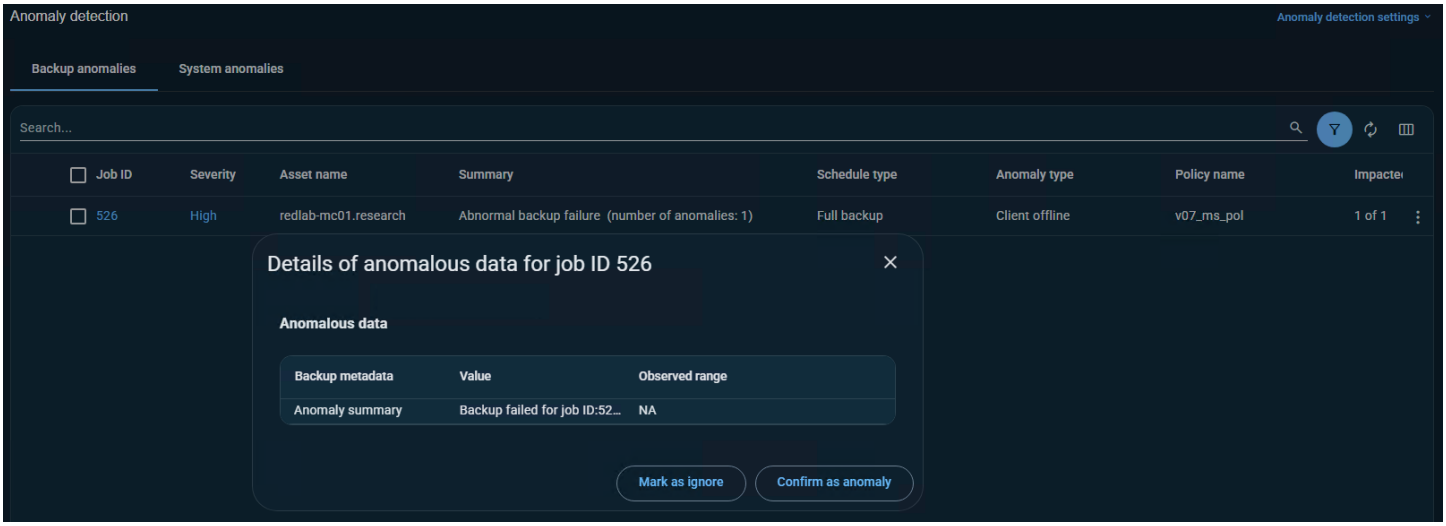
Name	Date modified	Type	Size
791g8ha668946x475128959q39s4bt5z79n...	4/20/2026 11:50 AM	-ENCRYPTED File	46 KB
ai.3gd6h7e.-encrypted	4/20/2026 11:50 AM	-ENCRYPTED File	1,360 KB
c804pyle3l1576ler88c40211cjzply1t34vftr7...	4/20/2026 11:50 AM	-ENCRYPTED File	19,531,266 ...
d.323876rge.-encrypted	4/20/2026 11:50 AM	-ENCRYPTED File	740 KB
di53gtil3qs3yeunb5u7282225g34a3mi8jb...	4/20/2026 11:50 AM	-ENCRYPTED File	195,317 KB
h50s8mk2w9o1897o169095l164g916es4s0...	4/20/2026 11:50 AM	-ENCRYPTED File	89 KB
how_to_decrypt.txt	4/20/2026 11:49 AM	Text Document	1 KB
k8f3frlaj6n95e.le.-encrypted	4/20/2026 11:50 AM	-ENCRYPTED File	8,920 KB
lj37o8400xa72p20wzenlq0.92rn61ge.-encr...	4/20/2026 11:50 AM	-ENCRYPTED File	202 KB
r718708uqkprnv9ok46cnhf1f.uh4mpm27...	4/20/2026 11:50 AM	-ENCRYPTED File	100,239 KB
trial-recovery.1.6e.-encrypted	4/20/2026 11:50 AM	-ENCRYPTED File	215 KB
trial-recovery.1dvg4a04az51700urhh5aqe...	4/20/2026 11:50 AM	-ENCRYPTED File	416 KB
trial-recovery.1ocncu54fww17754002ntp...	4/20/2026 11:50 AM	-ENCRYPTED File	137 KB
trial-recovery.2i040ieh1f4cz1191o8895419...	4/20/2026 11:50 AM	-ENCRYPTED File	13 KB
trial-recovery.2p1rcgdh70a1aq9si8nhxcx3...	4/20/2026 11:50 AM	-ENCRYPTED File	278 KB
trial-recovery.2x442x9505epvps4l10h0k84...	4/20/2026 11:50 AM	-ENCRYPTED File	1,297 KB
trial-recovery.3el7ub5c7340dd736dr5212...	4/20/2026 11:50 AM	-ENCRYPTED File	3,652 KB
trial-recovery.3hl4ll3vu5g1y0oggz.n77dze...	4/20/2026 11:50 AM	-ENCRYPTED File	12 KB
trial-recovery.3mub7a1ei6egv4gtn42201a...	4/20/2026 11:50 AM	-ENCRYPTED File	120 KB
trial-recovery.3qxc8q36lq4.o3a7e.-encryp...	4/20/2026 11:50 AM	-ENCRYPTED File	156 KB

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



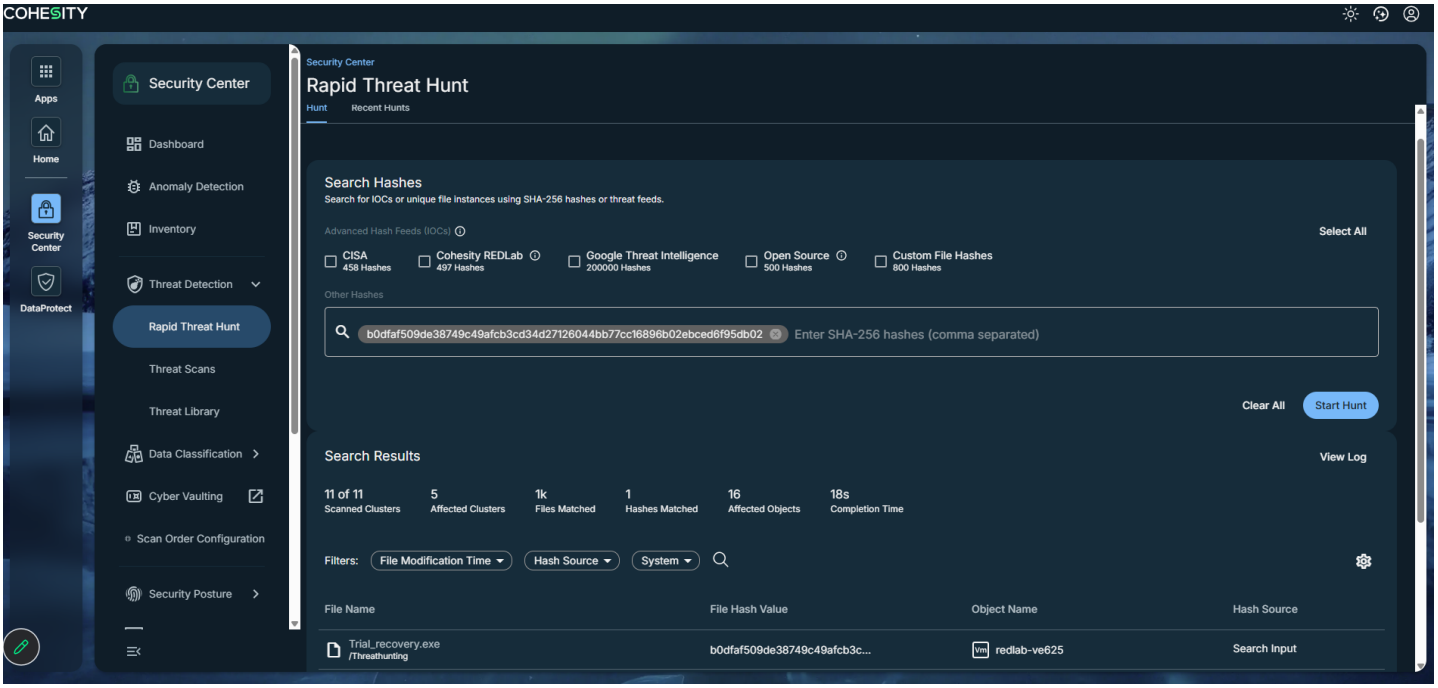
Protection & Detection Outcomes

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 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 Trial_recovery 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.

Payload Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Native API	T1106	Execution
Shared Modules	T1129	Execution
Hooking	T1179	Persistence, Privilege Escalation, Stealth
Create or Modify System Process	T1543	Persistence, Privilege Escalation, Stealth
Process Injection	T1055	Privilege Escalation, Stealth
Obfuscated Files or Information	T1027	Stealth
Software Packing	T1045	Stealth
Indicator Removal	T1070	Stealth
File Deletion	T1107	Stealth
Indirect Command Execution	T1202	Stealth
Impair Defenses	T1562	Stealth
Input Capture	T1056	Credential Access, Collection
System Service Discovery	T1007	Discovery

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

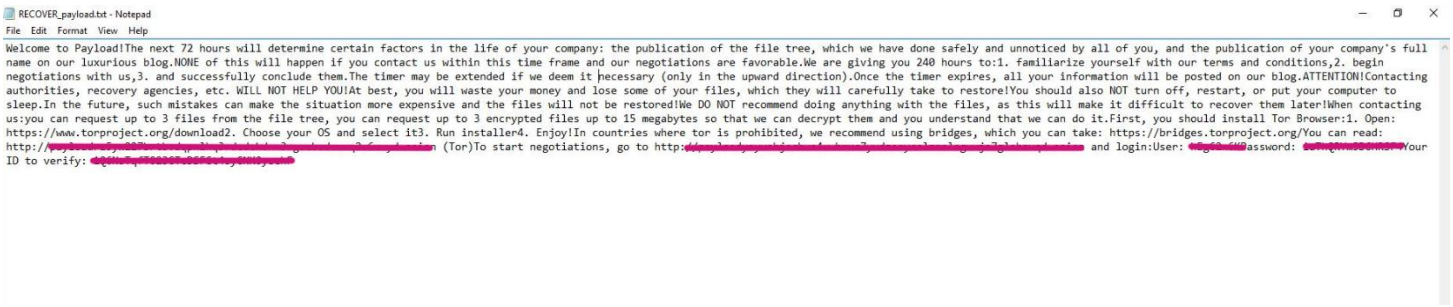
Malware impact post execution

Payload ransomware performs targeted file encryption across local disks, network-accessible shares, and virtualized environments, including VMware ESXi hosts. The ransomware enumerates user data, application files, backups, and virtual machine disk images prior to encryption, ensuring broad operational impact across both endpoint and server workloads. Encrypted files are renamed with the ".payload" extension. It employs a strong hybrid cryptographic scheme inspired by the leaked Babuk ransomware source code. Following encryption, Payload drops a ransom note "RECOVER_payload.txt" in affected directories. Victims are directed to a Tor-based negotiation portal and threatened with public disclosure of exfiltrated data if ransom demands are not met.

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

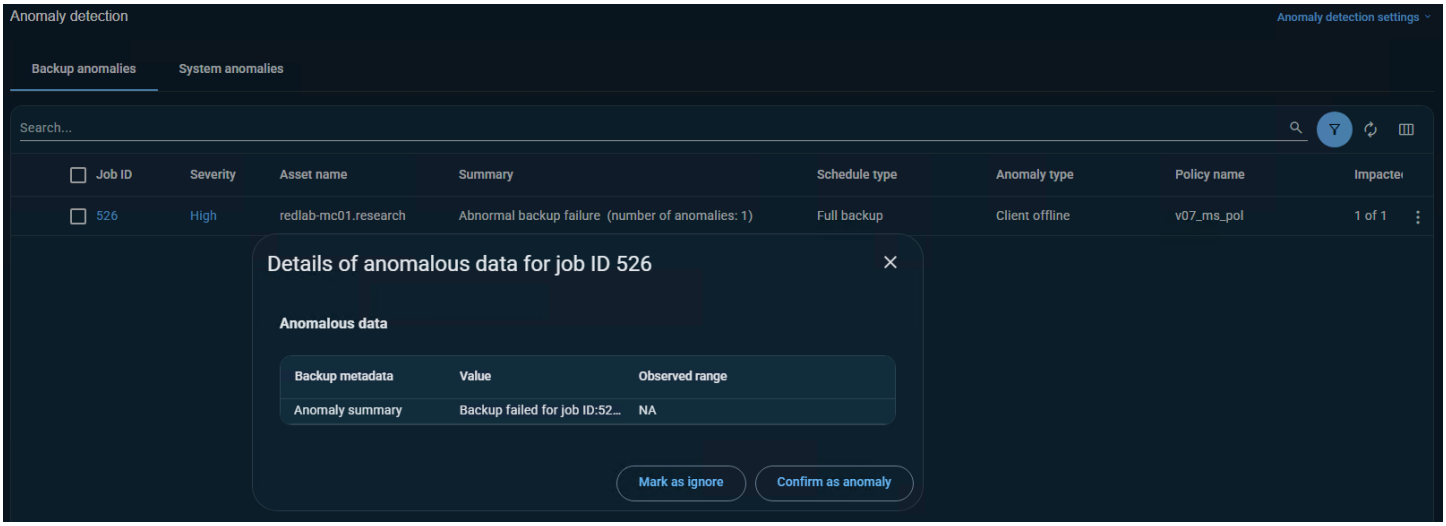
Name	Date modified	Type	Size
2021-AI-Index-Report_Master.pdf.payload	4/27/2026 3:36 AM	PAYLOAD File	13,905 KB
3903fe18c342c0a1ed83917e283d1314 (1).jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	45 KB
3903fe18c342c0a1ed83917e283d1314.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	45 KB
4411.doc.payload	4/27/2026 3:36 AM	PAYLOAD File	883 KB
23277.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	277 KB
2514219.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	506 KB
83538686.webp.payload	4/27/2026 3:36 AM	PAYLOAD File	34 KB
1633199491-1633199490440.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	151 KB
6369653753837926326Ah9yH.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	134 KB
6369653753837926326vinSA.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	122 KB
abdc_journal_list_05122018-csv.xls.payload	4/27/2026 3:36 AM	PAYLOAD File	736 KB
AHQ Data File 2016.xls.payload	4/27/2026 3:36 AM	PAYLOAD File	1,356 KB
Altja_jõgi_Lahemaal.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	4,870 KB
anom_data.zip.payload	4/27/2026 3:36 AM	PAYLOAD File	93 KB
AQAR-2019-2020.pdf.payload	4/27/2026 3:36 AM	PAYLOAD File	357 KB
BabyElephantWalk60.wav.payload	4/27/2026 3:36 AM	PAYLOAD File	2,585 KB
background-park-wonder-famous-countryside-waterscape_1417-1105.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	1,095 KB
beautiful-rain-forest-ang-ka-nature-trail-doi-inthanon-national-park-thailand-36703721.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	182 KB
beutiful-indian-peacock-on-tree-260nw-2031028856.webp.payload	4/27/2026 3:36 AM	PAYLOAD File	35 KB
Blending-Handling-Bulletin-Final.pdf.payload	4/27/2026 3:36 AM	PAYLOAD File	3,129 KB
Btech_CivilFT_RegA.doc.payload	4/27/2026 3:36 AM	PAYLOAD File	2,378 KB
c4d5c1db2688b9da8dd1a9fd22bd17d2.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	116 KB
CantinaBand3.wav.payload	4/27/2026 3:36 AM	PAYLOAD File	130 KB
CantinaBand60.wav.payload	4/27/2026 3:36 AM	PAYLOAD File	2,585 KB
ClassAutoSearchTraffic.pdf.payload	4/27/2026 3:36 AM	PAYLOAD File	482 KB
CSE-2018_04_24.doc.payload	4/27/2026 3:36 AM	PAYLOAD File	2,433 KB
CV-Europass-A.M-29.09.2021.doc.payload	4/27/2026 3:36 AM	PAYLOAD File	274 KB
Cyber-Handbook-Enterprise.pdf.payload	4/27/2026 3:37 AM	PAYLOAD File	8,916 KB
download.jpg.payload	4/27/2026 3:36 AM	PAYLOAD File	8 KB

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



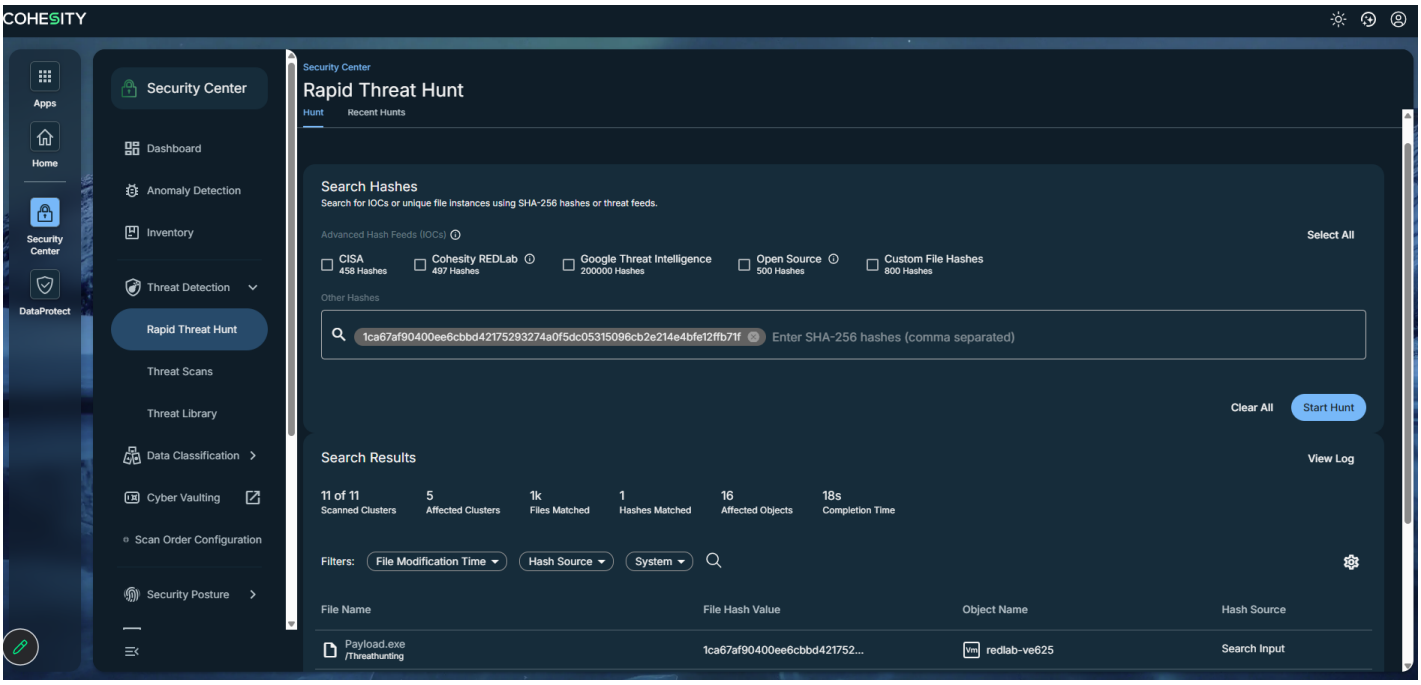
Protection & Detection Outcomes

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 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 Payload 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 VanHelsing ransomware strain.

- While in case of Find, Trial_recovery and Payload 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