

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.

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: KryBit Family: Babuk (Sodinokibi-style)	dab06e47581b87c21699bb1126b7cb2370cf86d069ad25b9b86cff8e450d7e29
Name: Zawoo Family: Zawoo Ransomware Group	dd21e22e2c4fffc5939dc6e42ee42ed497138d17245b59dcf4b0aca9739e337e
Name: The Gentlemen Family: The Gentlemen Group	51b9f246d6da85631131fcd1fabf0a67937d4bdd e33625a44f7ee6a3a7baebd2
Name: DeadLock Family: DeadLock Ransomware Family	3c1b9df801b9abbb3684670822f367b5b8cda566b749f457821b6481606995b3

KryBit Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Data Destruction	T1485	Impact
Process Injection	T1055	Defense Evasion, Privilege Escalation
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Masquerading	T1036	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Application Layer Protocol	T1071	Command and Control
Data Staged	T1074	Collection
File and Directory Discovery	T1083	Discovery
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
System Owner/User Discovery	T1033	Discovery

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

Malware impact post execution

KryBit was selected for this month's report on the strength of its sustained activity and growing regional relevance. The group has accumulated roughly 147 confirmed victims to date, including a peak of 36 disclosures in August 2026 alone — an average of about 24 per month. Targeted sectors span manufacturing, healthcare, construction, transportation, financial services, education, government and technology.

KryBit is a 32-bit Windows PE payload (GUI subsystem) that was scored at 'Critical' severity level under REDLab analysis. Static signatures matched the Babuk code lineage, while its runtime behaviour and the recovery artifacts it writes align with the Sodinokibi/REvil instruction-file pattern, indicating a payload assembled from well-established ransomware building blocks rather than an entirely novel family.

Before encrypting, the sample profiles the host extensively. It queries the keyboard layout, system locale and language registry keys – resolves volume mount points and historical removable and network drive entries, reads the volume serial number and physical hardware ID for victim profiling, enumerates running processes and checks its own token for administrator or UAC elevation status. A date-expiration check and a SetUnhandledExceptionFilter anti-debug hook were both observed, and the process created a hidden window to keep the activity off-screen.

Encryption is broad and destructive. The strain systematically walks user directories with wildcards, opens a large number of files requesting WRITE or DELETE access, and strips file attributes to defeat read-only protection before writing. Every affected file is renamed with a ".KRYBIT" extension, and REDLab analysis recorded mass file deletion and overwriting of existing files alongside the encryption activity. A single ransom note filename, "RECOVER-README", is copied across every affected directory, and the Recycle Bin is manipulated during the run.

For command and control and anti-recovery, KryBit issued HTTP requests carrying features characteristic of malware traffic, including a request to a commonly exploitable directory path, and generated network activity that fell outside the monitored API log. It also attempted to delete or modify volume shadow copies and invoked Windows utilities to carry out parts of the routine indirectly. The ransom note lists four Tor blog addresses and asserts that confidential and sensitive data was exfiltrated before encryption, confirming a double-extortion posture.

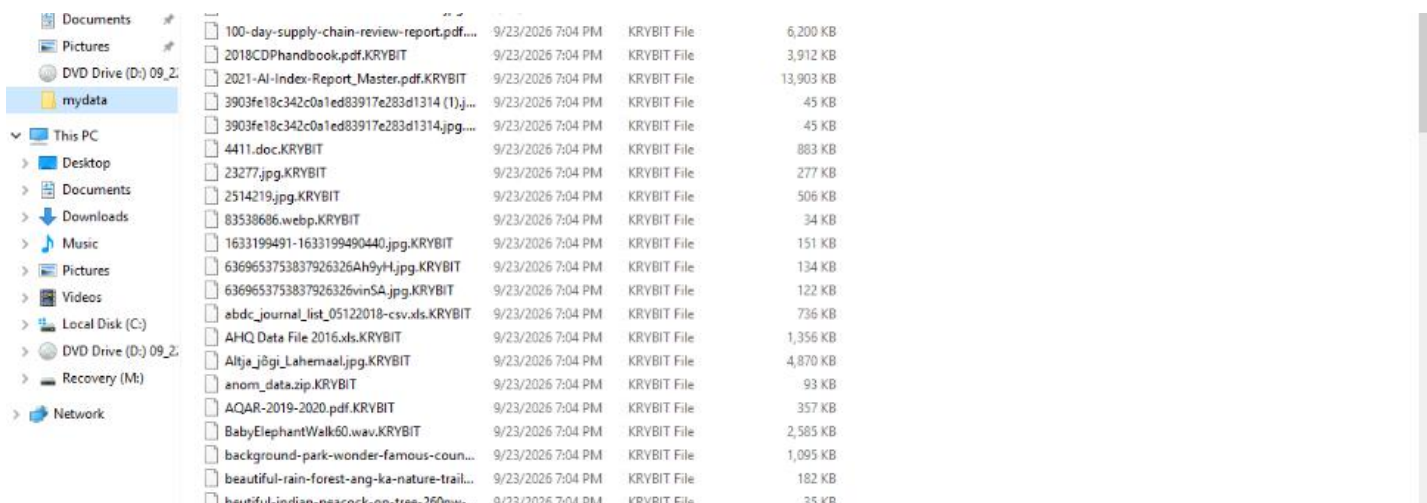


Figure 1: Victim files following detonation, each appended with the “.KRYBIT” extension.

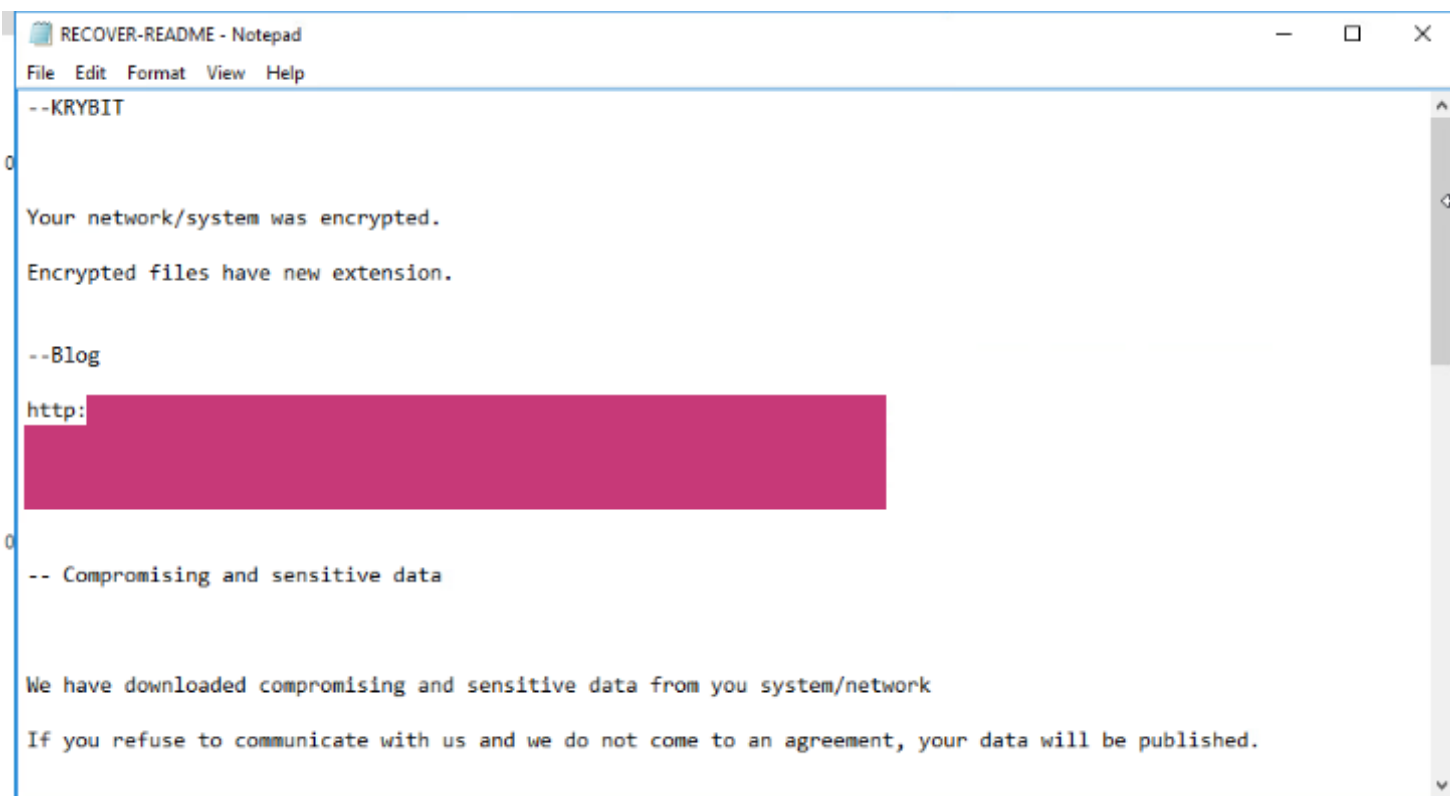


Figure 2: The “RECOVER-README” ransom note confirming encryption and listing the attacker’s Tor blog addresses.

Protection & Detection Outcomes

Both DataProtect and NetBackup delivered 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: KryBit 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 KryBit ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

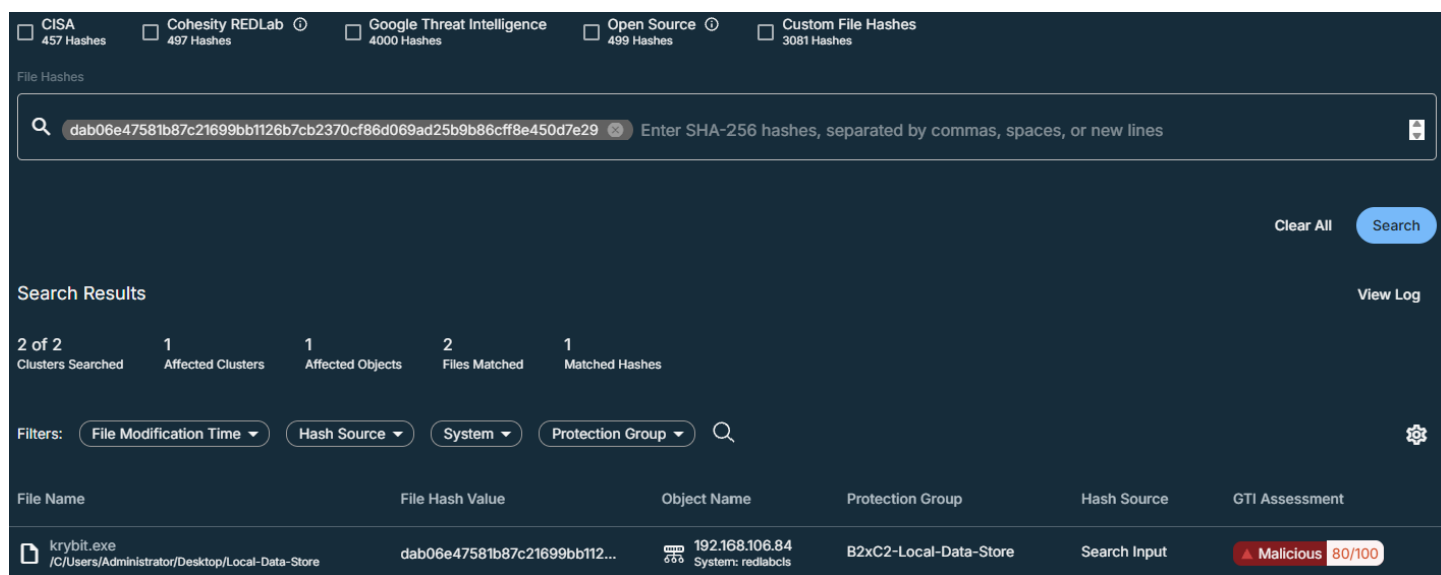


Figure 4: KryBit Rapid Threat Hunt Result.

Zawoo Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Data Destruction	T1485	Impact
Bootkit	T1542.003	Defense Evasion, Persistence
Indicator Removal	T1070	Defense Evasion
Process Injection	T1055	Defense Evasion, Privilege Escalation
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Obfuscated Files or Information	T1027	Defense Evasion
Software Packing	T1027.002	Defense Evasion
Masquerading	T1036	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
OS Credential Dumping	T1003	Credential Access
Credentials from Web Browsers	T1555.003	Credential Access
Credentials In Files	T1552.001	Credential Access
Data from Local System	T1005	Collection
Data Staged	T1074	Collection
Native API	T1106	Execution
Application Layer Protocol	T1071	Command and Control
Replication Through Removable Media	T1091	Initial Access, Lateral Movement

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

Malware impact post execution

Zawoo was selected as a newly active group whose encryption behaviour breaks conventional detection assumptions. 22 victim organisations were disclosed within roughly one month of the group's emergence. Victims span Germany, New Zealand, France, Brazil, Czech Republic, Austria and Canada, including a coordinated attack cluster in August 2026. Rather than appending a recognisable encrypted-file extension, Zawoo replaces the entire original filename and extension with random characters, and its double-extortion model includes threats to email stolen data directly to victims' customers rather than posting it to a leak site.

Zawoo is a 64-bit Windows PE console payload. It is packed, carries an unknown PE section name and a suspicious PDB path, and was the most functionally complete strain evaluated this month - combining credential theft, raw disk access and direct syscall evasion with conventional mass encryption.

The strain opens with layered environment checks: keyboard layout and locale queries, language checks via the registry, mouse-movement detection, a date-expiration timeout, service enumeration for anti-virtualization purposes and a SetUnhandledExceptionFilter anti-debug hook. It executes direct syscalls to bypass EDR and user-land API hooks, tries to unhook monitored Windows functions, and creates a process in a suspended state before reading and writing into the memory of other processes. Inter-process coordination was observed through named mutexes and shared memory mappings.

Encryption is aggressive and paired with heavy anti-recovery activity. The strain enumerates user directories with wildcards, opens a large number of files for WRITE or DELETE access, strips file attributes to bypass read-only restrictions, and both deletes and overwrites existing files. Affected files are renamed entirely - original filenames are replaced by opaque hexadecimal strings with a victim-specific extension (".NNAOFNYS" in this detonation) - and file-extension hijacking registry keys are modified so the renamed files resolve to the attacker's handler. A ransom note, "How To Restore Your Files", is dropped across affected directories. The sample then deleted volume shadow copies, cleared Windows event logs, created an autorun.inf file to propagate via removable media, and deleted its own binary from disk.

The ransom note is unusually long and negotiation-focused: it claims prior intrusion across the network, offers security consulting as part of the settlement, discourages contacting law enforcement, and provides a Session ID and an onionmail address for contact.

	2E08D935F08149B8	9/23/2026 8:26 PM	NNAOFNYS File	85 KB
	2E96FDD6E358416A	9/23/2026 8:26 PM	NNAOFNYS File	130 KB
	2F0F367B0CF34553	9/23/2026 8:26 PM	NNAOFNYS File	90 KB
	2F78C02EDD4CAEAB	9/23/2026 8:26 PM	NNAOFNYS File	52 KB
	03EBEC6873B05693	9/23/2026 8:26 PM	NNAOFNYS File	28 KB
D:) 09_2:	3A8A34D4D69095AB	9/23/2026 8:26 PM	NNAOFNYS File	34 KB
	3ABD384E6BCDC3F0	9/23/2026 8:26 PM	NNAOFNYS File	130 KB
	3B1AFF729519BDC3	9/23/2026 8:26 PM	NNAOFNYS File	116 KB
	3FFCA9718DDAB17F	9/23/2026 8:26 PM	NNAOFNYS File	1,060 KB
	4AE8D9A89675487F	9/23/2026 8:26 PM	NNAOFNYS File	217 KB
	4B44725428B2E47F	9/23/2026 8:26 PM	NNAOFNYS File	62 KB
	4DA36BFD38DDC3E	9/23/2026 8:26 PM	NNAOFNYS File	823 KB
	5B5F8C94F9FE7343	9/23/2026 8:26 PM	NNAOFNYS File	107 KB
	06D661D154F80914	9/23/2026 8:26 PM	NNAOFNYS File	42 KB
	6E1FDA94E775E699	9/23/2026 8:26 PM	NNAOFNYS File	21 KB
(C:)	6E467F41AB02A68B	9/23/2026 8:26 PM	NNAOFNYS File	277 KB
D:) 09_2:	6E92496580B677A1	9/23/2026 8:26 PM	NNAOFNYS File	1,293 KB
	7A7F8CE27836773A	9/23/2026 8:26 PM	NNAOFNYS File	12 KB
	7D04B34FB046231D	9/23/2026 8:26 PM	NNAOFNYS File	53 KB
	8B7C849F5A1B3ACF.NnaOfnYs	9/23/2026 8:27 PM	MXVF0_F File	8,916 KB
	8EAB95CEC3CCCAD3	9/23/2026 8:26 PM	NNAOFNYS File	182 KB

Figure 5: Victim files renamed to opaque hexadecimal strings and appended with the victim-specific “.NNAOFNYS” extension.

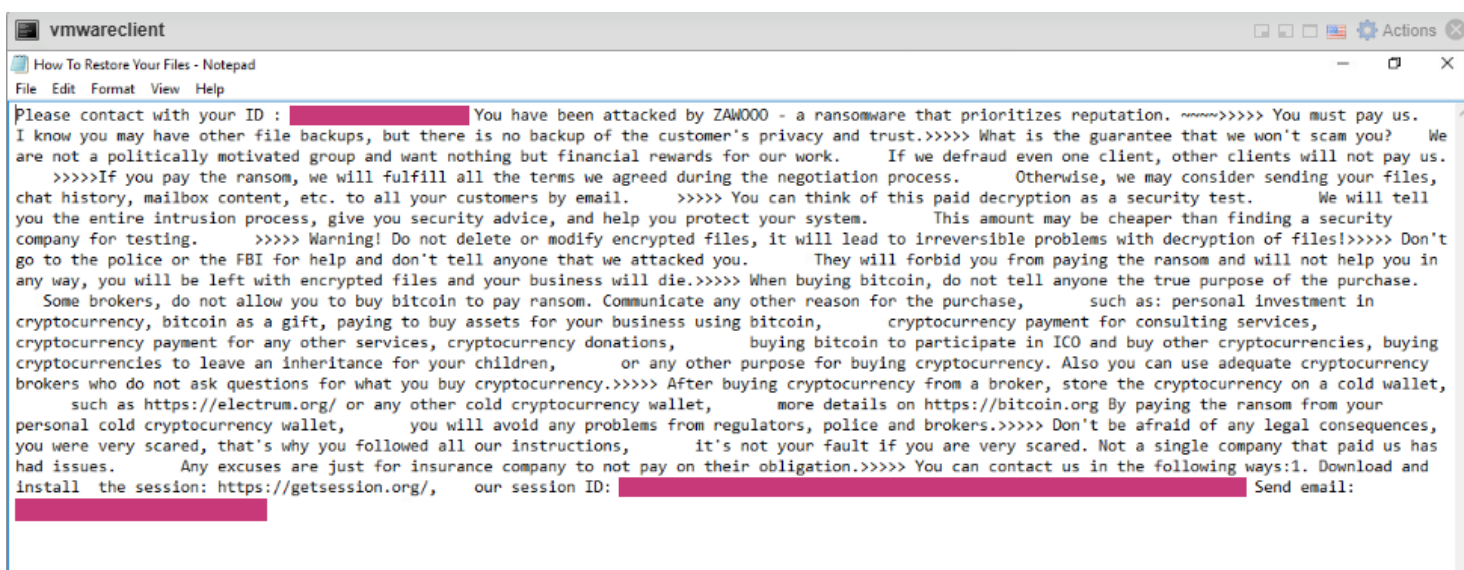


Figure 6: The “How To Restore Your Files” ransom note, claiming full intrusion of the network and directing the victim to a Session ID and onionmail address.

Protection & Detection Outcomes

Both DataProtect and NetBackup delivered 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.

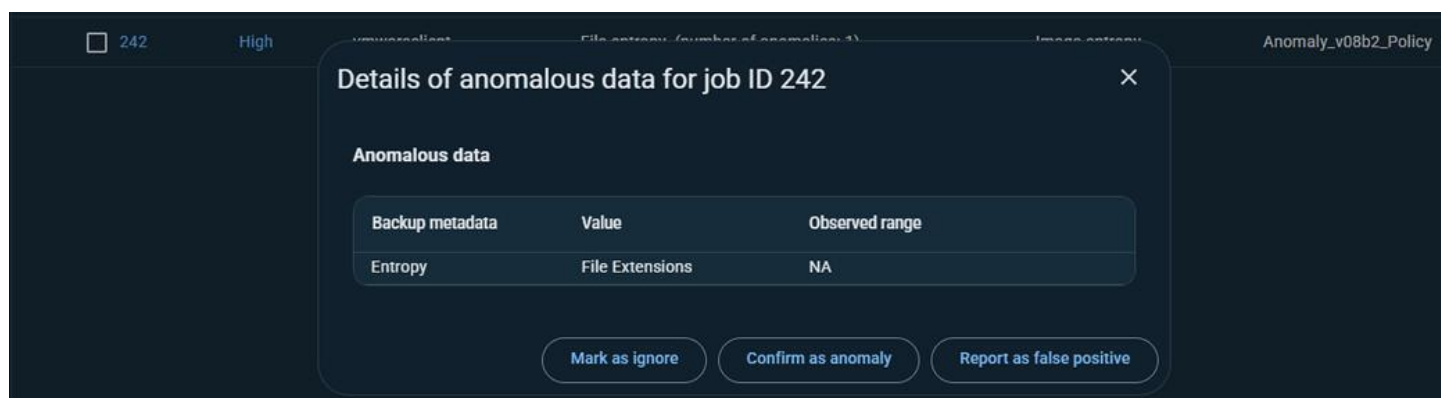


Figure 7: Zawoo Entropy Anomaly Result.

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

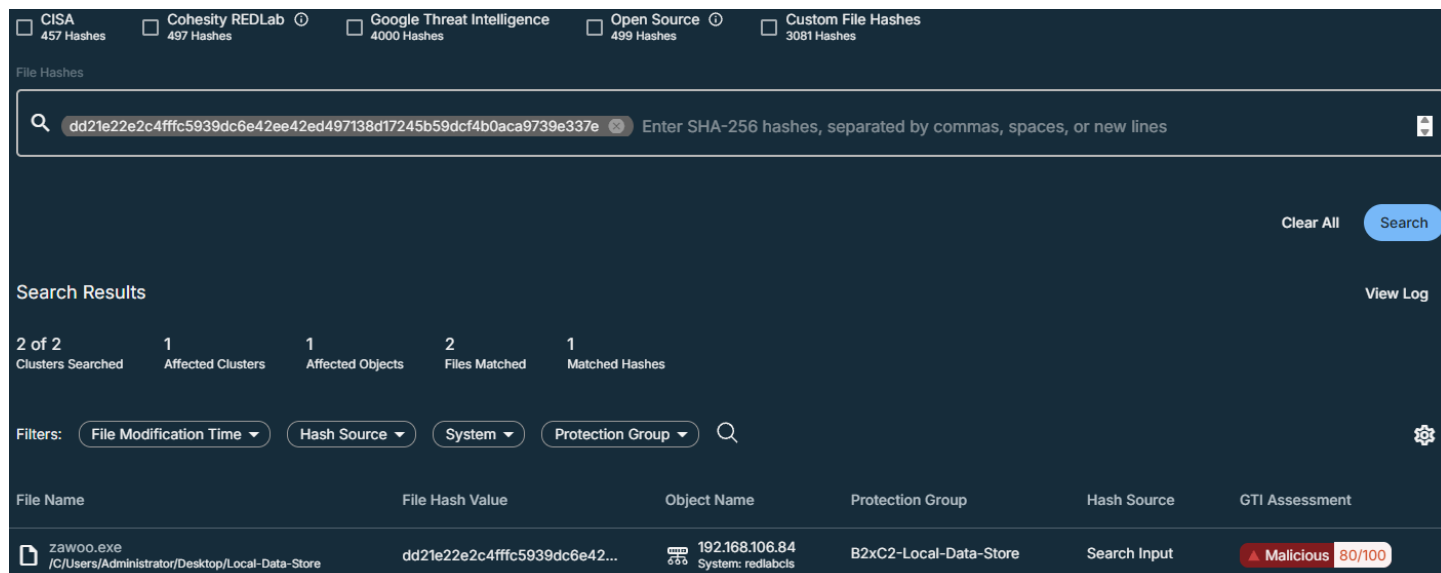


Figure 8: Zawoo Rapid Threat Hunt Result.

The Gentlemen Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Inhibit System Recovery	T1490	Impact
Service Stop	T1489	Impact
Internal Defacement	T1491.001	Impact
Impair Defenses	T1562	Defense Evasion
Disable or Modify Tools	T1562.001	Defense Evasion
Clear Windows Event Logs	T1070.001	Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Software Packing	T1027.002	Defense Evasion
Process Injection	T1055	Defense Evasion, Privilege Escalation
Hijack Execution Flow	T1574	Defense Evasion, Persistence, Privilege Escalation
Command and Scripting Interpreter: PowerShell	T1059.001	Execution
Windows Management Instrumentation	T1047	Execution
System Services: Service Execution	T1569.002	Execution
Remote Services: SMB/Windows Admin Shares	T1021.002	Lateral Movement
Lateral Tool Transfer	T1570	Lateral Movement
Network Share Discovery	T1135	Discovery

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

Malware impact post execution

The Gentlemen was selected as the largest active ransomware campaign in the current landscape. It has accumulated approximately 870 disclosed victims across 32 countries, averaging around 58 disclosures per month and peaking at 145 in August 2026. The group targets enterprise backup infrastructure directly, including backup services and Volume Shadow Copies, and uses Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques to disable EDR and other security products ahead of encryption. Affected sectors include manufacturing, healthcare, financial services, government, education, retail, technology and construction.

The Gentlemen is a 64-bit Windows console payload written in Go. This strain was detonated inside the REDLab facility alongside the other strains this month; the assessment below is derived from REDLab analysis of the binary's runtime behaviour together with the ransom note and encrypted-file artifacts captured from the affected host.

The binary is packed, carries an unknown PE section name and high-entropy content, and registers a vectored exception handler to hijack execution flow. REDLab analysis also observed it creating RWX memory and probing high-memory ranges in a module-stomping pattern, along with routines that attempt to unhook or suspend the monitoring functions that detection tooling relies on - an explicit anti-analysis posture.

Cryptography is self-contained: the payload embeds ChaCha20 and AES (with AES-NI support) primitives, together with a custom hashing routine, so encryption proceeds without external dependencies. Affected files are renamed with a ".umc16h" extension, and a ransom note titled "README-GENTLEMEN.txt" is written for the victim.

The binary carries a broad operational toolkit rather than a single encryption routine. Static strings reveal command-line switches for spreading, share targeting, and "ultrafast" and "superfast" encryption modes, plus options to delay the main action and to suppress self-deletion. It embeds a PsExec service component for remote execution, builds PowerShell and WMI command lines to launch itself on remote computers, grants full access to created shares, enables the legacy SMB1 protocol, and registers a Defender process exclusion for itself. Anti-recovery and defence-impairment routines include volume shadow copy deletion, Windows event log clearing, Prefetch directory wiping, firewall modification and a large embedded kill list targeting database and enterprise application services. A "gentlemen.bmp" artifact indicates wallpaper defacement after encryption completes. The ransom note confirms double extortion. It states that confidential and business data, explicitly including NAS and cloud data, has been exfiltrated, and threatens publication on a leak site and reporting to data protection regulators. Contact is offered over Tox and Session, with a Tor leak blog and a 239-hour reveal timer.

83538686.webp.umc16h	8/17/2026 3:08 PM	UMC16H File	34 KB
1633199491-1633199490440.jpg.umc16h	8/17/2026 3:08 PM	UMC16H File	151 KB
6369653753837926326Ah9yH.jpg.umc16h	8/17/2026 3:08 PM	UMC16H File	134 KB
6369653753837926326vinSA.jpg.umc16h	8/17/2026 3:08 PM	UMC16H File	122 KB
abdc_journal_list_05122018-csv.xls.umc16h	8/17/2026 3:08 PM	UMC16H File	736 KB
AHQ Data File 2016.xls.umc16h	8/17/2026 3:08 PM	UMC16H File	1,356 KB
Altja_jögi_Lahemaal.jpg.umc16h	8/17/2026 3:08 PM	UMC16H File	4,870 KB
anom_data.zip.umc16h	8/17/2026 3:08 PM	UMC16H File	93 KB
AQAR-2019-2020.pdf.umc16h	8/17/2026 3:08 PM	UMC16H File	357 KB
BabyElephantWalk60.wav.umc16h	8/17/2026 3:08 PM	UMC16H File	2,585 KB
background-park-wonder-famous-coun...	8/17/2026 3:08 PM	UMC16H File	1,095 KB
beautiful-rain-forest-ang-ka-nature-trail...	8/17/2026 3:08 PM	UMC16H File	182 KB
beutiful-indian-peacock-on-tree-260nw-...	8/17/2026 3:08 PM	UMC16H File	35 KB
Blending-Handling-Bulletin-Final.pdf.u...	8/17/2026 3:08 PM	UMC16H File	3,129 KB
Btech_CivilFT_RegA.doc.umc16h	8/17/2026 3:08 PM	UMC16H File	2,378 KB
c4d5c1db2688b9da8dd1a9fd22bd17d2.jp...	8/17/2026 3:08 PM	UMC16H File	116 KB
CaptainDad2.wmv.umc16h	8/17/2026 3:08 PM	UMC16H File	120 KB

Figure 9: Victim files following encryption, each appended with the “.umc16h” extension.

README-GENTLEMEN.txt - Notepad

File Edit Format View Help

[REDACTED] = YOUR ID

Gentlemen, your network has been encrypted.

1. Any modification of encrypted files will make recovery impossible.
2. Only our unique decryption key and software can restore your files.
Brute-force, RAM dumps, third-party recovery tools are useless.
It's a fundamental mathematical reality. Only we can decrypt your data.
3. Law enforcement, authorities, and “data recovery” companies will NOT help you.
They will only waste your time, take your money, and block you from recovering your files – your business will be lost.
4. Any attempt to restore systems, or refusal to negotiate, may lead to irreversible wipe of all data and your network.
5. We have exfiltrated all your confidential and business data (including NAS, clouds, etc).
If you do not contact us, it will be published on our leak site and distributed to major hack forums and social networks.
In addition, it will be reported to the relevant data protection authorities and regulators.
This may result in official investigations, significant fines, and reputational damage for your company.
6. We guarantee 100% file recovery to their original state, bit by bit.
To demonstrate the quality of our work, you can provide two sample files, and we will restore them free of charge.

TOX CONTACT - RECOVER YOUR FILES

Contact us (add via TOX ID): [REDACTED]

Download Tox messenger: <https://tox.chat/download.html>

Contact us (add via Session ID): [REDACTED]

Download Session <https://getsession.org>

CONTACT TO PREVENT DATA LEAK (7 DAYS BEFORE YOUR COMPANY DATA WILL BE PUBLISHED IN OUR BLOG, WITH 239 HOURS REVEAL TIMER)

Check our blog: [REDACTED]

Download Tor browser: <https://www.torproject.org/download/>

Follow us on X: <https://x.com/TheGentlemen25>

Any other means of communication are fake and may be set up by third parties.
Only use the methods listed in this note or on the specified website.

Figure 10: The “README-GENTLEMEN.txt” ransom note claiming exfiltration of NAS and cloud data, with Tox and Session contact details and a leak-site reveal timer.

Protection & Detection Outcomes

Both DataProtect and NetBackup delivered 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: The Gentlemen 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 Gentlemen ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

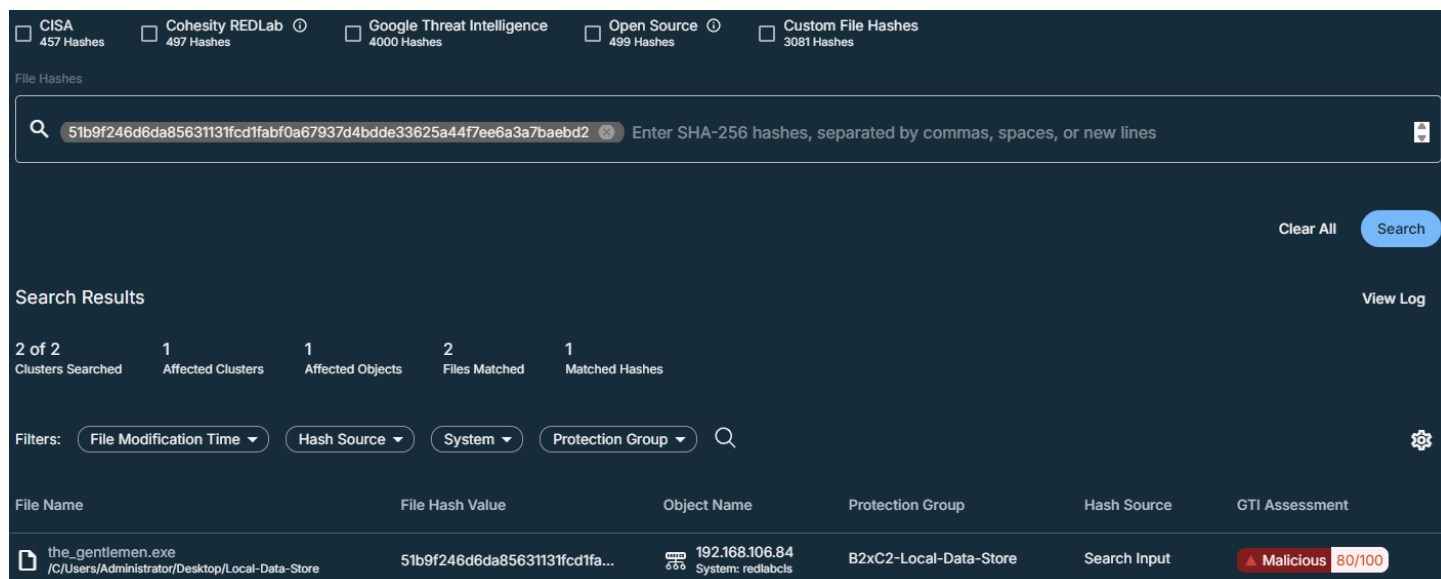


Figure 12: The Gentlemen Rapid Threat Hunt Result.

DeadLock Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Service Stop	T1489	Impact
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Windows Service	T1543.003	Persistence, Privilege Escalation
Bootkit	T1542.003	Defense Evasion, Persistence
Impair Defenses	T1562	Defense Evasion
Disable or Modify Tools	T1562.001	Defense Evasion
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Hide Artifacts	T1564	Defense Evasion
Masquerading	T1036	Defense Evasion
Application Layer Protocol	T1071	Command and Control
Replication Through Removable Media	T1091	Initial Access, Lateral Movement
Data Staged	T1074	Collection
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
System Owner/User Discovery	T1033	Discovery

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

Malware impact post execution

DeadLock was selected as an emerging threat built around novel extortion infrastructure. Between roughly 96 and 101 confirmed victims have been identified across some 40 countries, over half of them in Europe. The group operated quietly for approximately 11 months before entering the monthly victim leaderboard in second place during its first month of public disclosure. Backup and shadow copy services are named explicitly in the malware's own service-stop list, and the strain partially encrypts large files such as databases, VM images and backups while still rendering them unusable. Its extortion infrastructure is blockchain-hosted, leaving no domains or IP addresses to block or take down.

DeadLock is a 32-bit Windows PE console payload that was scored at 'Critical' severity level under REDLab analysis. Rather than relying on obfuscation, DeadLock distinguishes itself through persistence and service manipulation. The strain performs the now-familiar profiling sequence - keyboard layout and locale queries, language checks via the registry, token checks for administrator or UAC elevation status, volume mount point resolution, historical removable and network drive discovery, and volume serial number and hardware ID reads. It additionally queries display device information to determine whether it is running in a virtualized environment, and installs a SetUnhandledExceptionFilter anti-debug hook.

Persistence and impact are pursued in parallel. DeadLock exhibited service creation and modification techniques during the run, and the sample attempted to stop active services and terminate other processes on the host. It issued suspicious IO control codes indicative of disk enumeration or bootkit activity, and modified registry keys for file-extension hijacking so that renamed files resolve through the attacker's own handler. An autorun.inf file was created, giving the strain a route to propagate via removable media.

Encryption appends a victim-specific compound extension - ".F8C6A8.dlock" in this detonation - to every affected file, and a matching ransom note, "READ ME.F8C6A8.txt", is dropped for the victim. After encryption the desktop wallpaper is replaced with a full-screen notice reading "Your infrastructure DeadLocked - All Files stolen and encrypted", which also directs the victim to the note. The note itself claims military-grade encryption across documents, photos, videos and databases, offers a single-file decryption test capped at 1 MB, and accepts Bitcoin or Monero, with contact over Session.

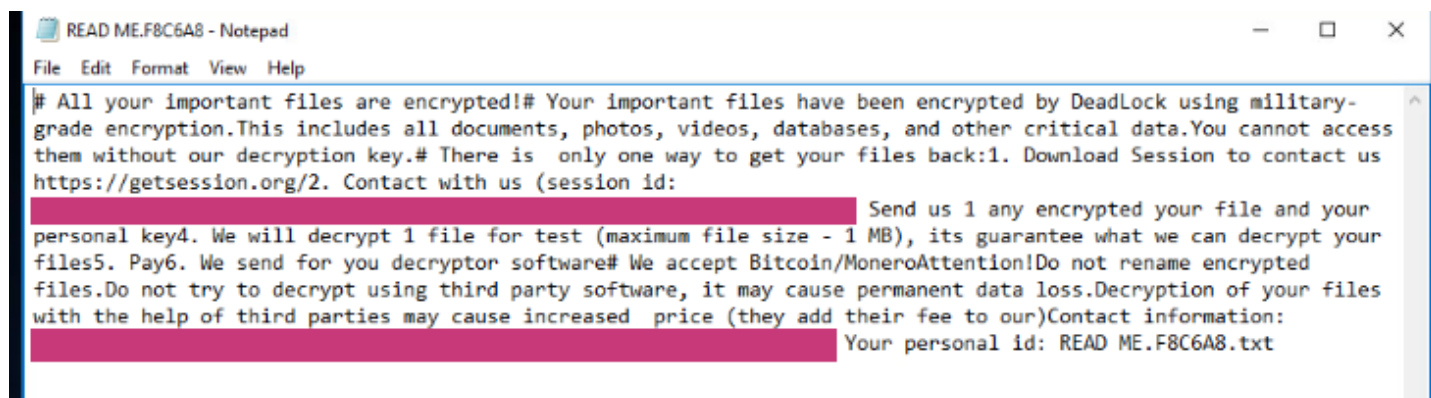


Figure 13: The “READ ME.F8C6A8.txt” ransom note claiming military-grade encryption.



Figure 14: Desktop wallpaper replaced after encryption with a full-screen notice claiming data theft and directing the victim to the ransom note.

Protection & Detection Outcomes

Both DataProtect and NetBackup delivered 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: DeadLock 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 DeadLock ransomware. The hunt successfully identified impacted clusters, objects, and file artifacts within the environment, providing clear visibility into the scope of compromise.

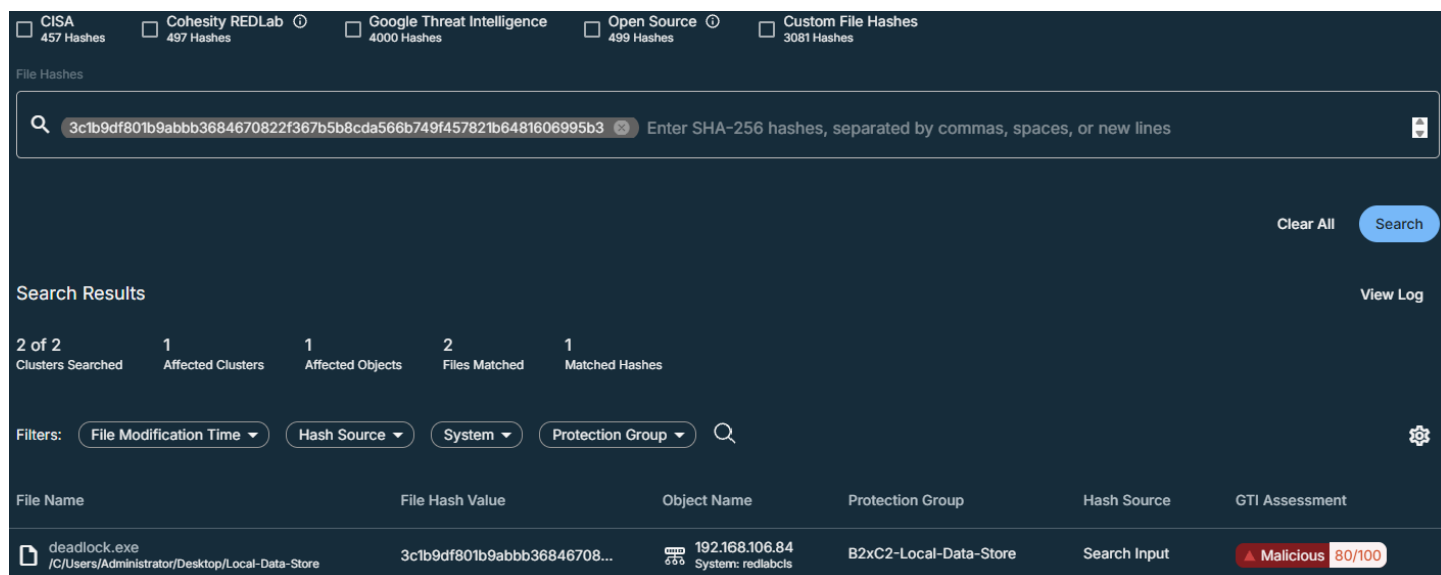


Figure 16: DeadLock Rapid Threat Hunt Result.

Summary

- Both DataProtect and NetBackup achieved successful VMware backup and recovery across all four ransomware strains tested this month – KryBit, Zawoo, The Gentlemen and DeadLock, 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 across all four strains - 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>