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 for assessing resilience against real-world cyber threats. This process enhances our understanding of malware techniques and tactics for crearing products that are effective in data protection and security. The insights gained also provide valuable guidance to customer 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 products 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: Kyber Family: Kyber Ransomware Family	4ed176edb75ae2114cda8cfb3f83ac2ecdc4476fa1ef30ad8c81a54c0a223a29
Name: VECT 2.0 Family: Vect Ransomware Family	e512d22d2bd989f35ebaccb63615434870dc0642b0f60e6d4bda0bb89adee27a
Name: Zollo Family: MedusaLocker Ransomware Family	54b2bfff73a73ac9115dce4018ba7bd4bdfa5bc0174be3f2d7491dfb829fa7f3
Name: ShinySp1d3r Family: ShinyHunters Ransomware Group	670a269d935f1586d4f0e5bed685d15a38e6fa790f763e6ed5c9fdd72dce3cf2

Kyber Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Scripting	T1064	Execution
Native API	T1106	Execution
Shared Modules	T1129	Execution
Modify Registry	T1112	Persistence
Pre-OS Boot	T1542	Persistence, Stealth
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Access Token Manipulation	T1134	Privilege Escalation, Stealth
Abuse Elevation Control Mechanism	T1548	Privilege Escalation
Obfuscated Files or Information	T1027	Stealth
Masquerading	T1036	Stealth
Indicator Removal	T1070	Stealth
Indirect Command Execution	T1202	Stealth
Virtualization/Sandbox Evasion	T1497	Stealth, Discovery
Impair Defenses	T1562	Stealth
OS Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
System Service Discovery	T1007	Discovery

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

Malware impact post execution

Kyber emerged as one of the more technically intriguing ransomware strains in 2026 due to its claimed use of post-quantum cryptography within active ransomware operations. The malware was observed targeting both Windows and VMware ESXi environments in coordinated attacks, indicating a deliberate shift toward hypervisor-centric disruption. The Windows variant uses Kyber1024 + X25519 key exchange mechanisms, appends ".#~~~" extension post execution and drops ransom note named "READ_ME_NOW". Kyber's Rust-based modular architecture also hints at increasing ransomware industrialization and scalable RaaS development.

Image: Files encrypted post attack with ".#~~~" extension.

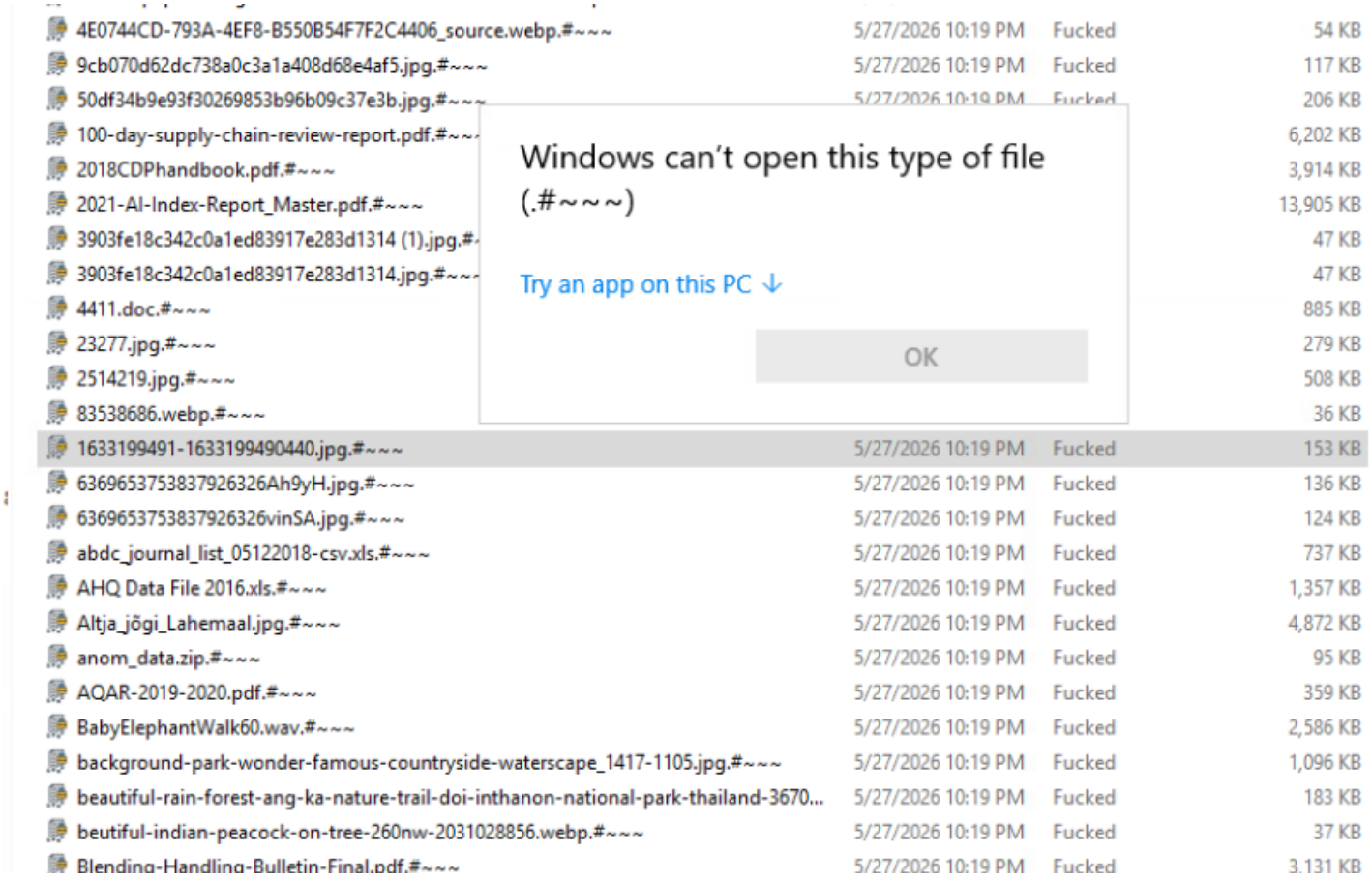
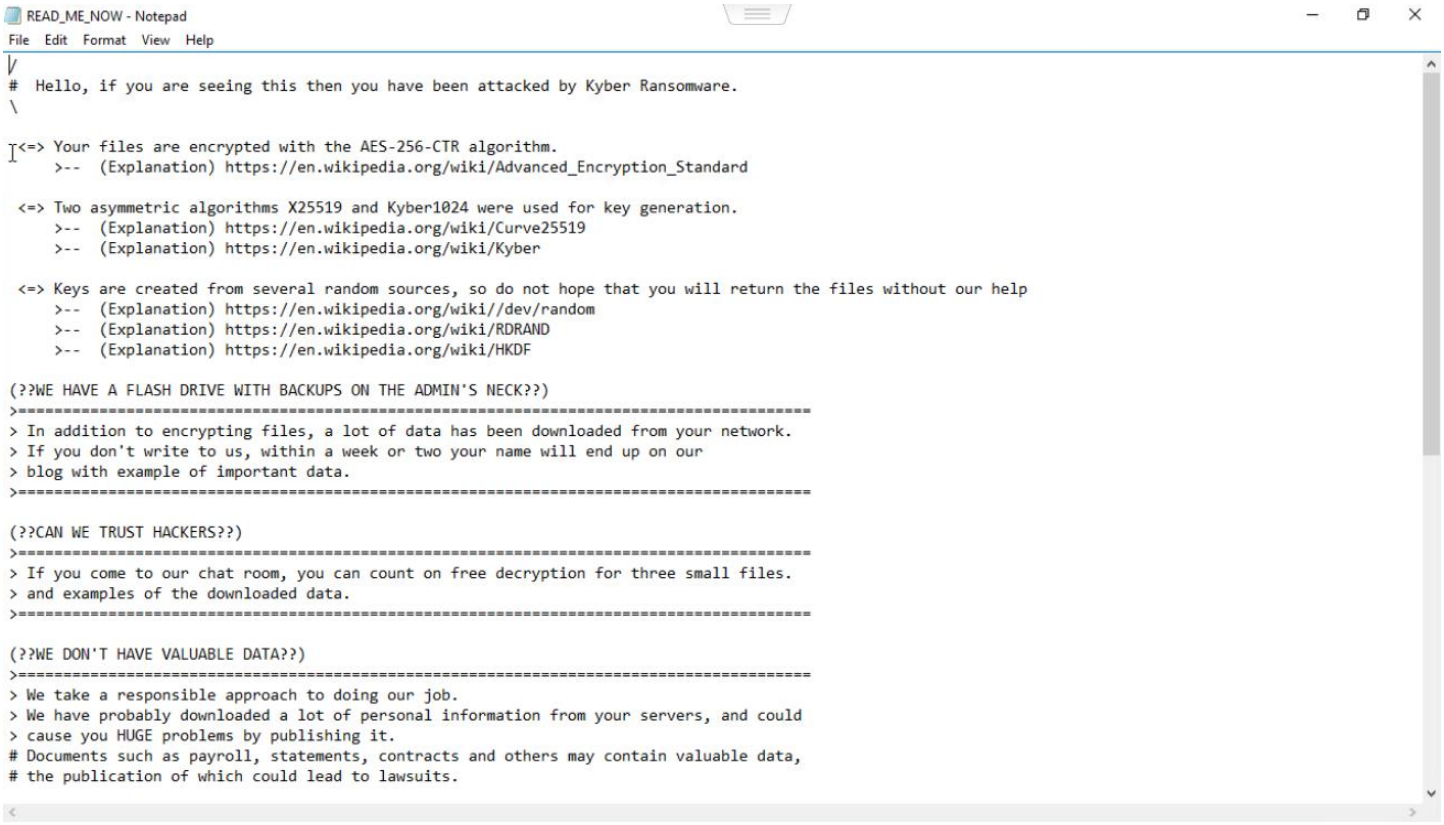
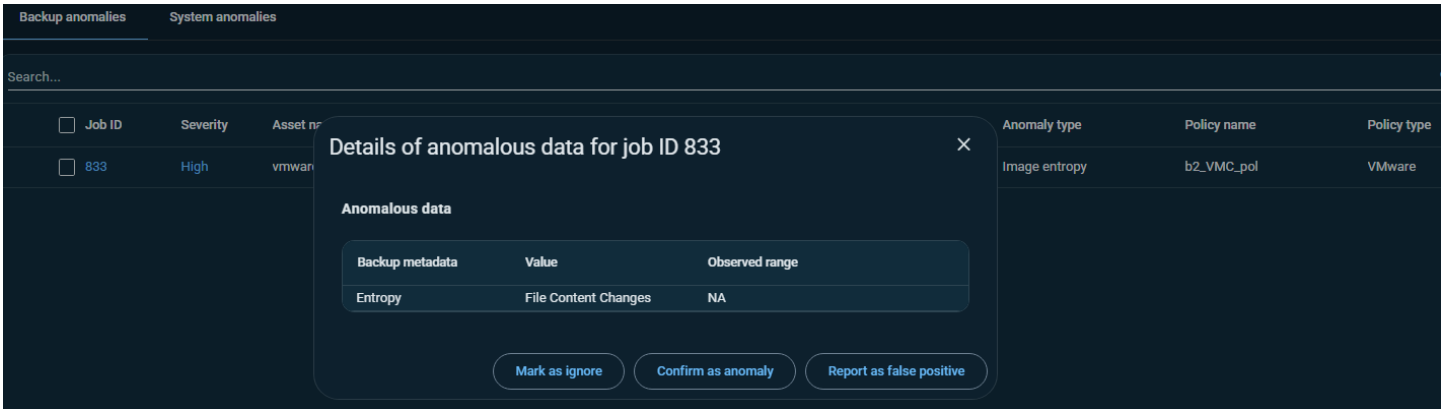


Image: Ransom Note named "READ_ME_NOW" dropped along with recovery details.



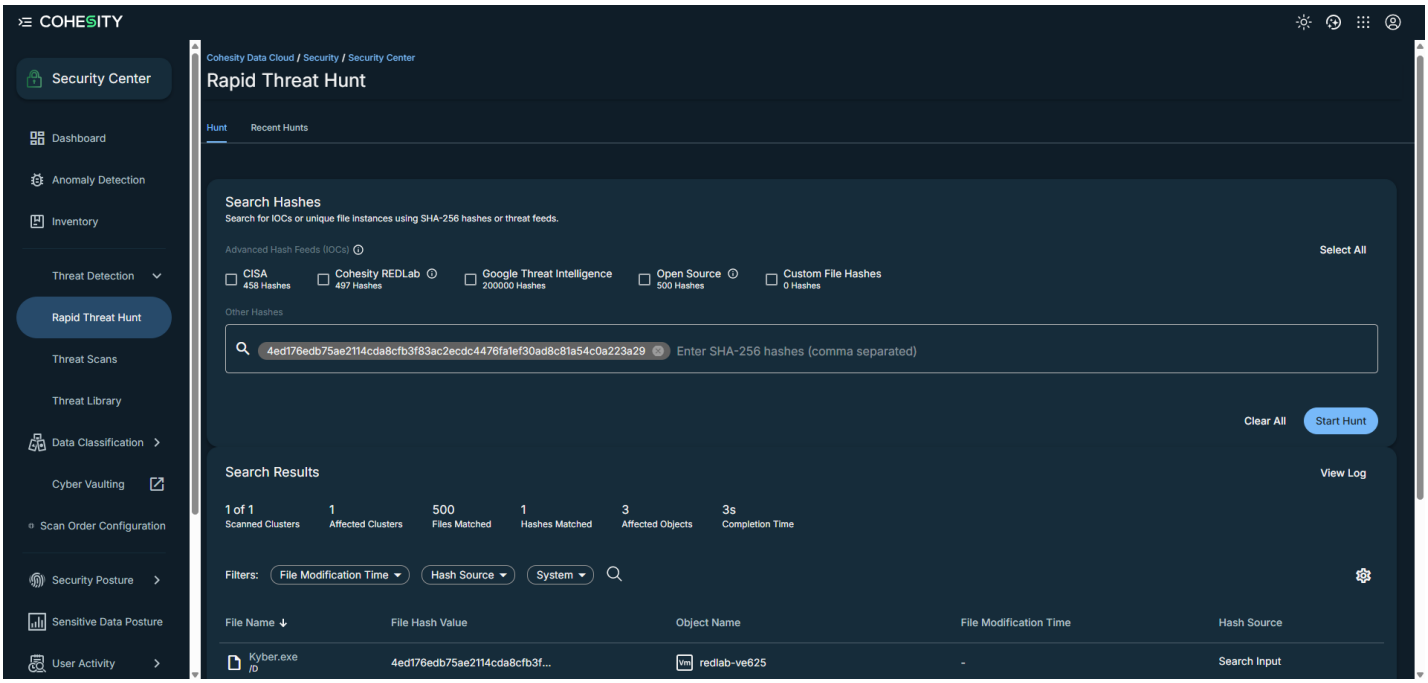
Protection & Detection Outcomes

After the attack, the DataProtect VMware backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully. Also, in the case of NetBackup an Image Entropy anomaly that detected unusual deviation in VMware backup job attributes 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 Kyber 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. DataProtect and NetBackup VMware based backup and recovery was successful.

VECT Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Scripting	T1064	Execution, Stealth
Shared Modules	T1129	Execution
Modify Registry	T1112	Persistence
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Process Injection	T1055	Privilege Escalation, Stealth
Obfuscated Files or Information	T1027	Stealth
Indicator Removal	T1070	Stealth
Indirect Command Execution	T1202	Stealth
Virtualization/Sandbox Evasion	T1497	Stealth, Discovery
Impair Defenses	T1562	Stealth
Hide Artifacts	T1564	Stealth
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
Native API	T1106	Execution
Shared Modules	T1129	Execution

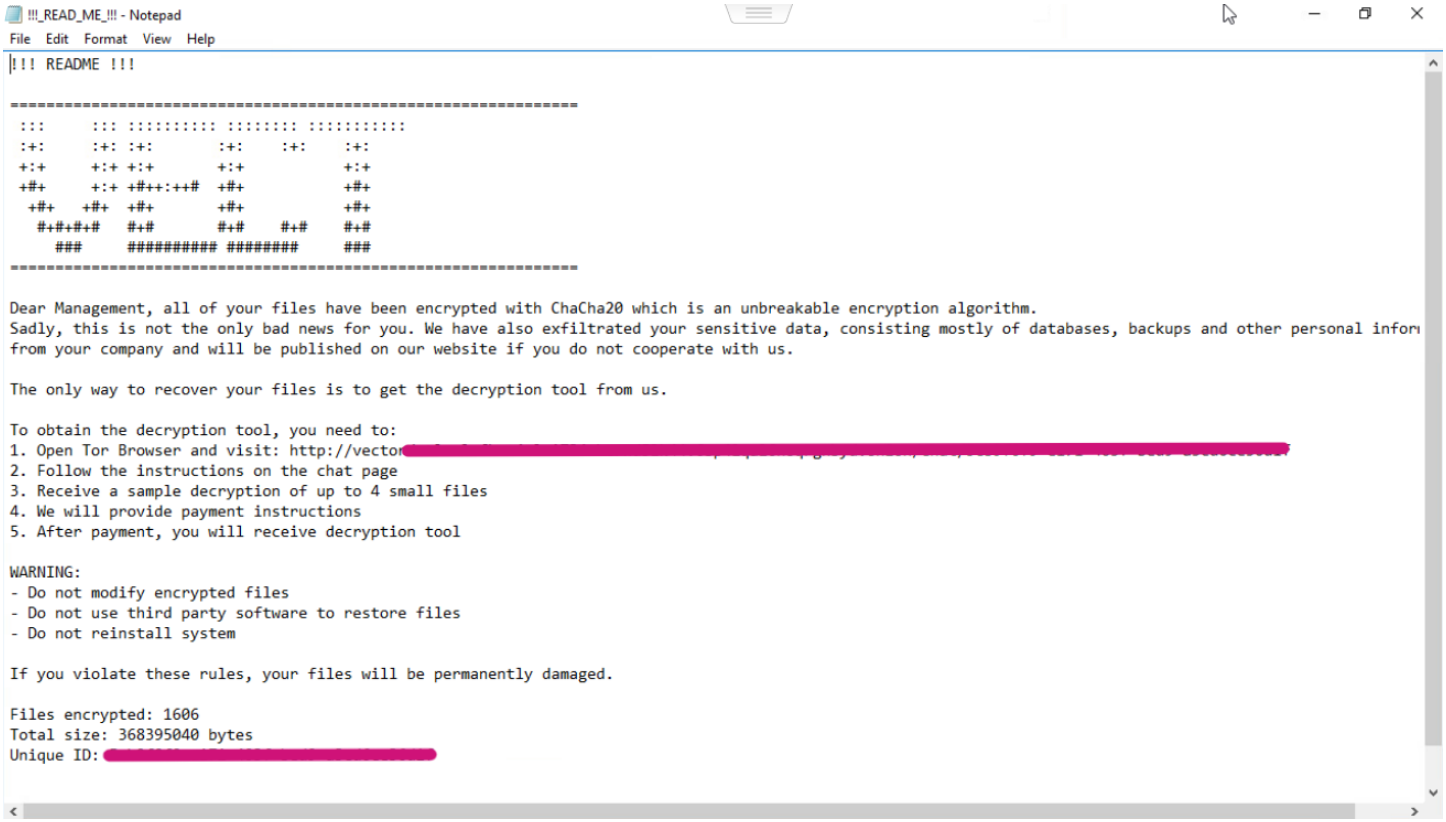
Note: Above table contains a curated subset of techniques prioritized for monitoring and response.*

Malware impact post execution

VECT ransomware emerged as one of the more unusual ransomware strains in late 2025 after researchers uncovered a critical flaw in its encryption logic that unintentionally renders large files permanently unrecoverable. The malware uses a multi-nonce ChaCha20 encryption mechanism during chunk-based file processing; however, only the final nonce is retained while earlier nonces are discarded entirely. As a result, files larger than approximately 131 KB cannot be fully decrypted even if attackers provide the correct decryption key, effectively transforming the ransomware into a destructive wiper. The flaw also reinforces the increasing importance of immutable and offline backups, as successful ransom negotiations may no longer guarantee data restoration.

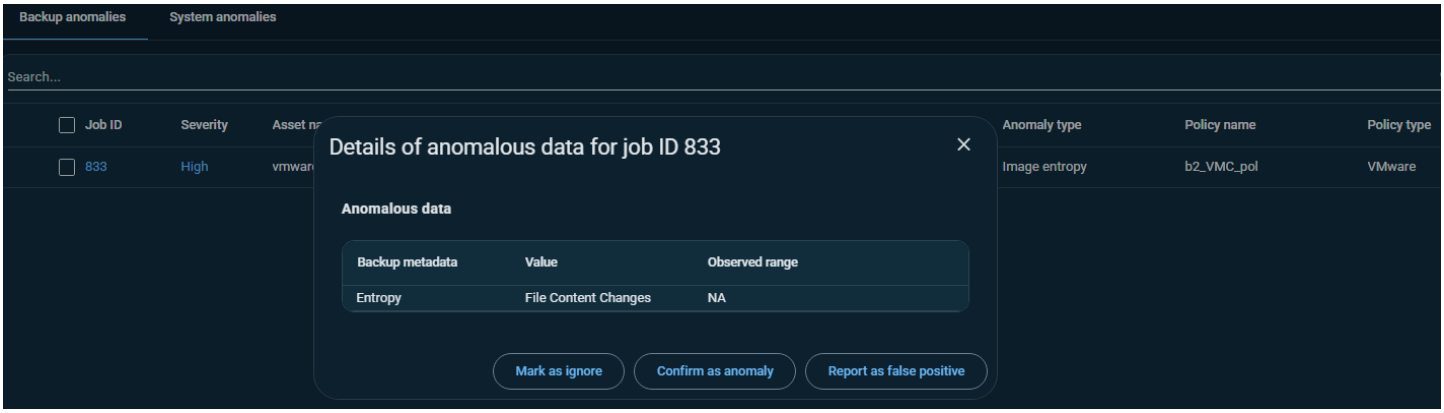
Image: Desktop Wallpaper updated post attack.

Image: Ransom Note named "!!!_READ_ME_!!!" dropped along with recovery details.



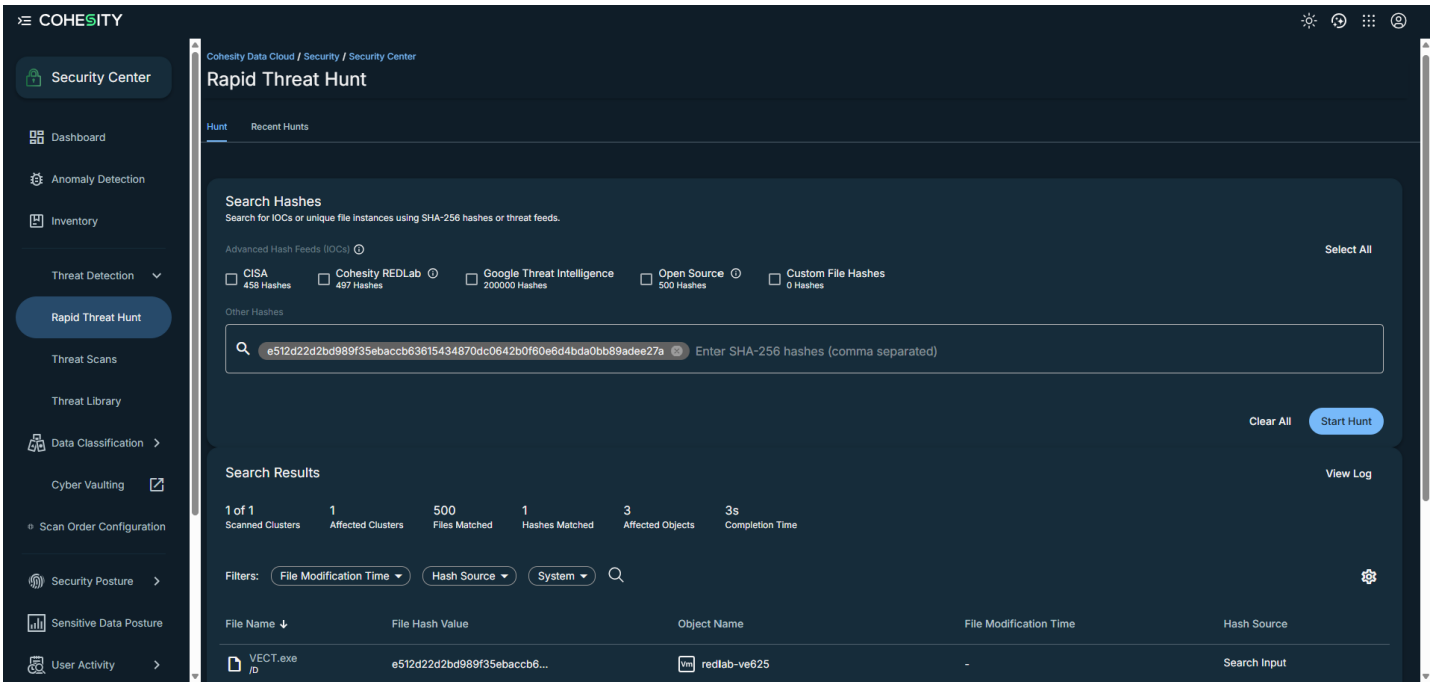
Protection & Detection Outcomes

After the attack, the DataProtect VMware backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully. Also, in the case of NetBackup an Image Entropy anomaly that detected unusual deviation in VMware backup job attributes 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 VECT 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. DataProtect and NetBackup VMware based backup and recovery was successful.

Zollo Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Command and Scripting Interpreter	T1059	Execution
Shared Modules	T1129	Execution
Modify Registry	T1112	Persistence, Defense Impairment
Pre-OS Boot	T1542	Persistence, Stealth
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Process Injection	T1055	Privilege Escalation, Stealth
Access Token Manipulation	T1134	Privilege Escalation, Stealth
Rootkit	T1014	Stealth
Obfuscated Files or Information	T1027	Stealth
Masquerading	T1036	Stealth
Indicator Removal	T1070	Stealth
Deobfuscate/Decode Files or Information	T1140	Stealth
Indirect Command Execution	T1202	Stealth
Virtualization/Sandbox Evasion	T1497	Stealth, Discovery
Hide Artifacts	T1564	Stealth
Hidden Window	T1143	Stealth
Indirect Command Execution	T1202	Stealth

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

Malware impact post execution

Zollo ransomware emerged as a newly identified variant within the MedusaLocker ransomware family and has recently been observed using hybrid RSA + AES encryption schemes combined with aggressive double-extortion tactics. Once executed, the malware encrypts victim files and appends extensions such as ".zollo6", ".zollo10" or other incrementing numeric variants depending on the campaign build. It also modifies the victim's desktop wallpaper and drops an HTML-based ransom note named "READ_NOTE.html," instructing victims to contact operators through rotating email infrastructure hosted on privacy-focused domains.

Image: Files encrypted post attack with ".zollo6" extension

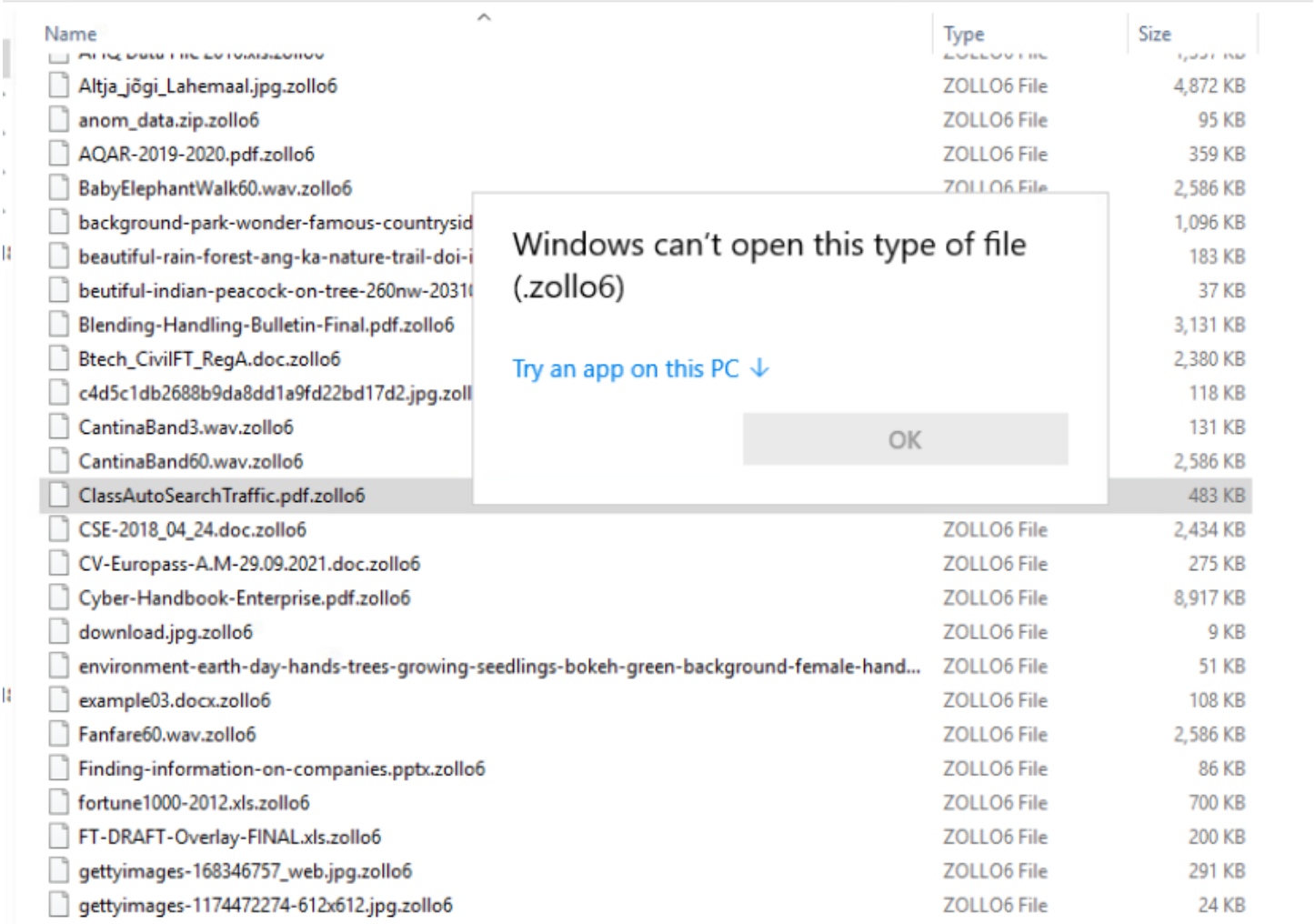
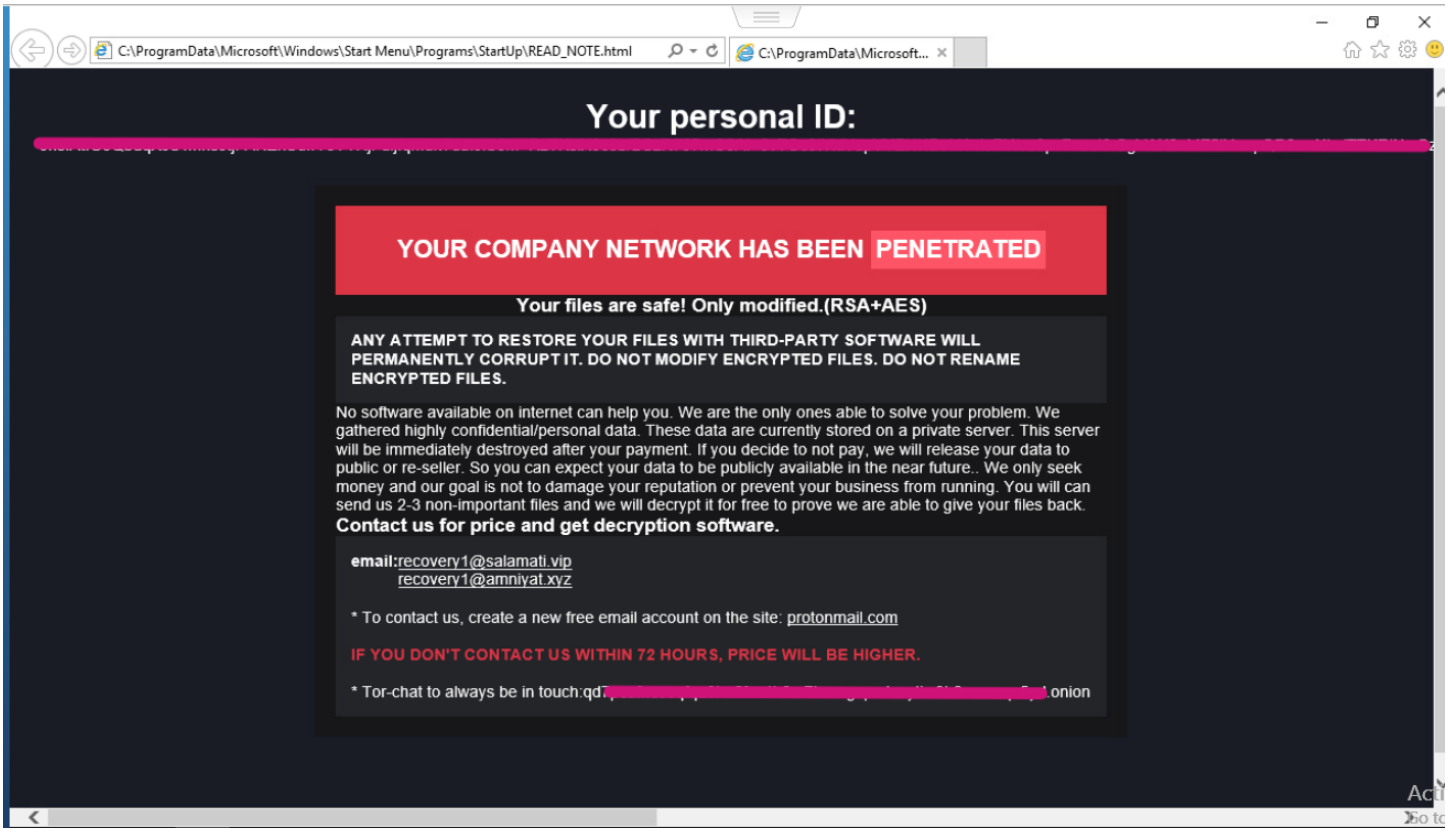
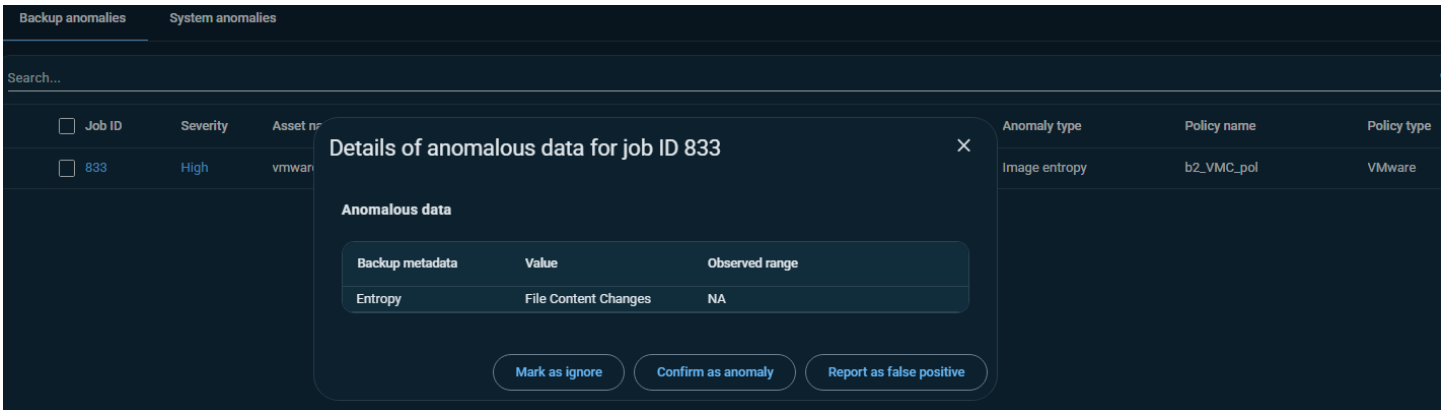


Image: Ransom Note named "READ_NOTE.html" dropped along with recovery details.



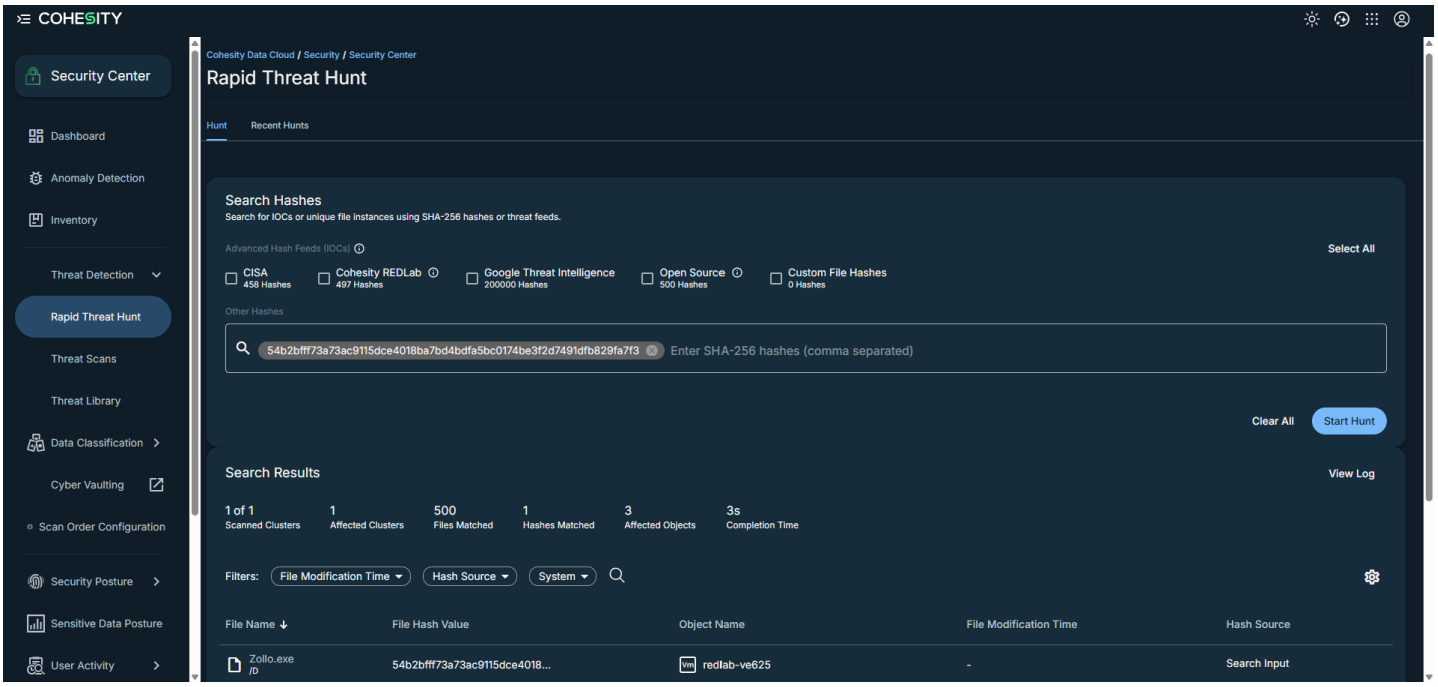
Protection & Detection Outcomes

After the attack, the DataProtect VMware backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully. Also, in the case of NetBackup an Image Entropy anomaly that detected unusual deviation in VMware backup job attributes 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 Zollo 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. DataProtect and NetBackup VMware based backup and recovery was successful.

ShinySp1d3r Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Shared Modules	T1129	Execution
Obfuscated Files or Information	T1027	Stealth
Masquerading	T1036	Stealth
Deobfuscate/Decode Files or Information	T1140	Stealth
Virtualization/Sandbox Evasion	T1497	Stealth, Discovery
OS Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Software Discovery	T1518	Discovery
Data from Local System	T1005	Collection
Email Collection	T1114	Collection
Data Encrypted for Impact	T1486	Impact

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

Malware impact post execution

ShinySp1d3r is a newly observed ransomware strain that gained significant traction in early 2026 due to its apparent operational overlap with ShinyHunters and Scattered Spider-style intrusion activity. Unlike traditional ransomware groups that primarily rely on malware deployment after exploiting vulnerabilities, ShinySp1d3r appears heavily focused on identity compromise, SaaS account takeover, MFA fatigue attacks, and helpdesk impersonation techniques for initial access and lateral movement. executed, the ransomware encrypts victim files using randomly generated extensions such as ".6s35eGh7", ".SubP8UXN", etc; changes the desktop wallpaper and drops a ransom note named "R3ADME_1Vks5fYe.txt". Ransom note instructs to contact operators through a private Tox messaging session to receive a decryptor and get recovery guidance, within the compromised environment.

Image: Files encrypted post attack with randomly generated extensions.

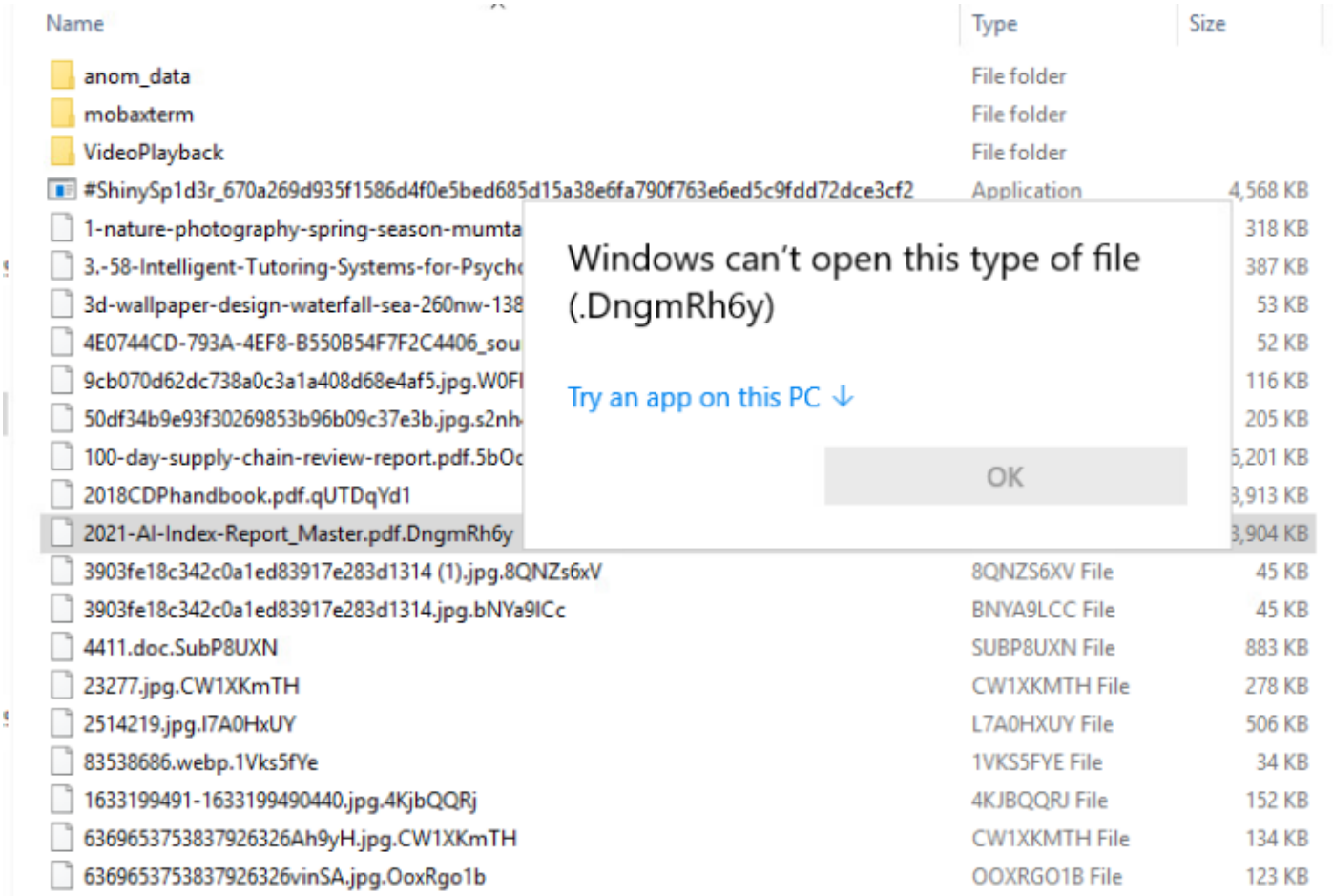
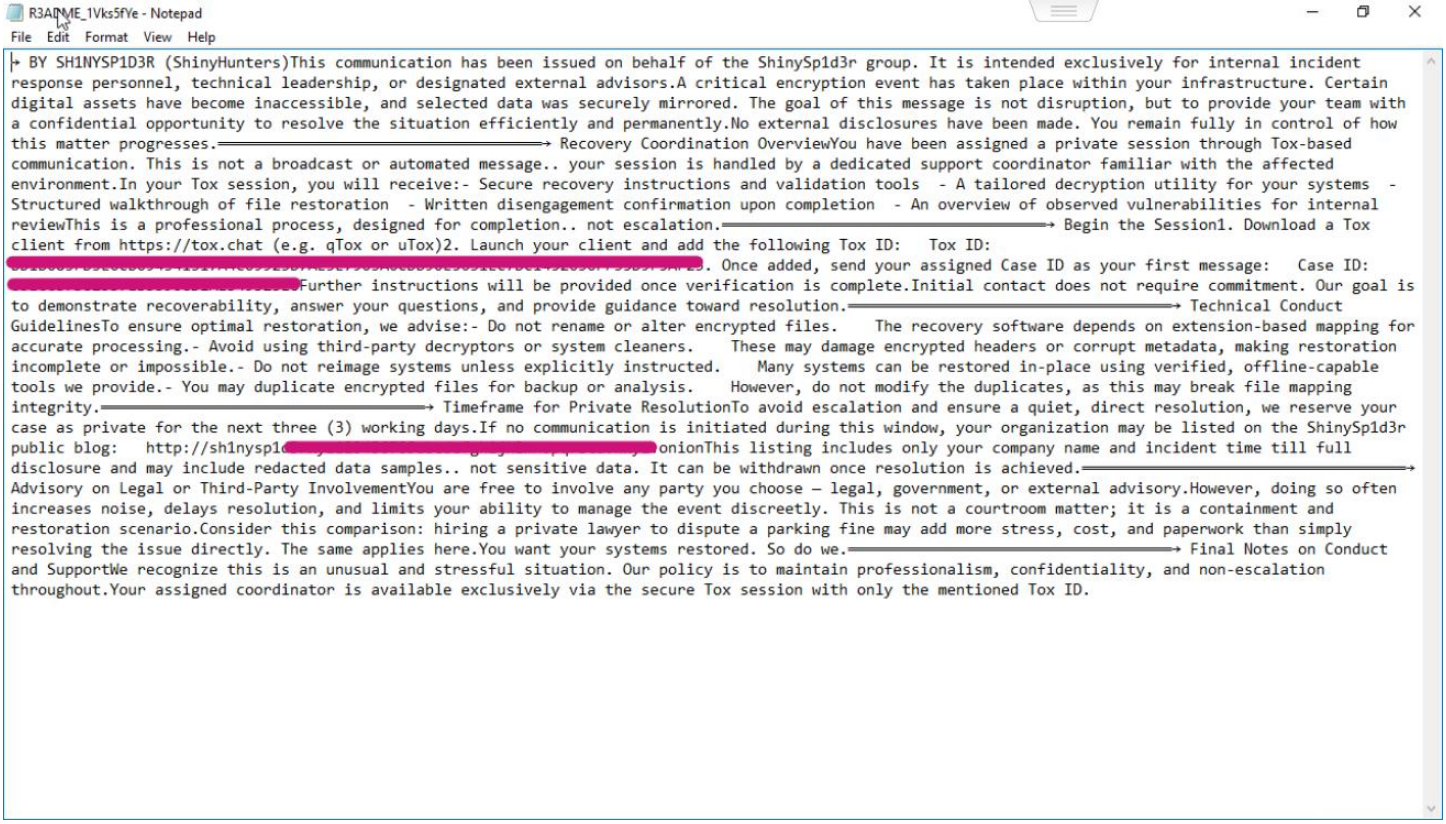


Image: Ransom Note named "R3ADME_1Vks5fYe.txt" dropped along with recovery details.



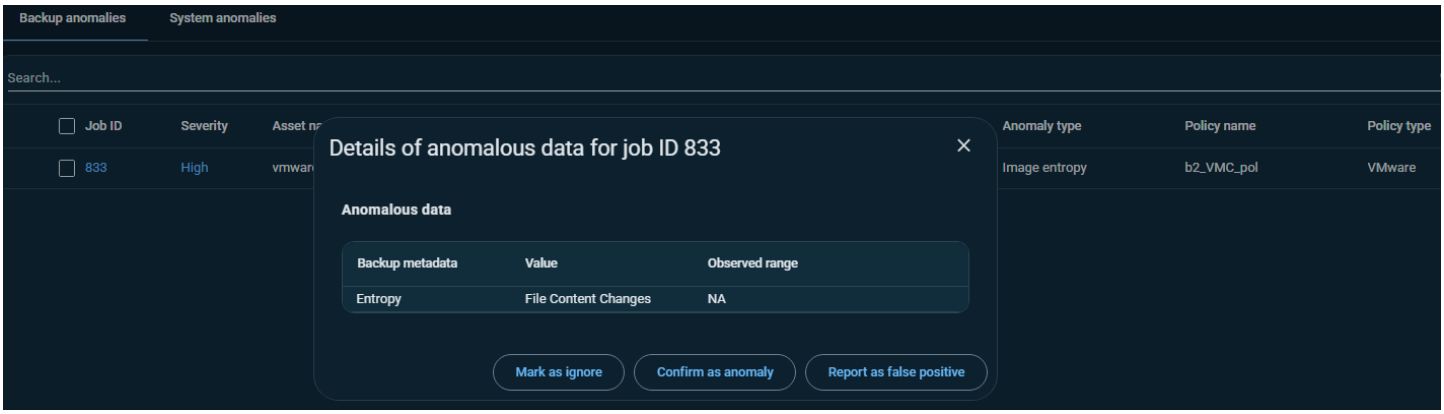
R3ADME_1Vks5fYe - Notepad

File Edit Format View Help

```
├ BY SH1NYSP1D3R (ShinyHunters)This communication has been issued on behalf of the ShinySp1d3r group. It is intended exclusively for internal incident
response personnel, technical leadership, or designated external advisors.A critical encryption event has taken place within your infrastructure. Certain
digital assets have become inaccessible, and selected data was securely mirrored. The goal of this message is not disruption, but to provide your team with
a confidential opportunity to resolve the situation efficiently and permanently.No external disclosures have been made. You remain fully in control of how
this matter progresses.═══════════════════════════════════════→ Recovery Coordination OverviewYou have been assigned a private session through Tox-based
communication. This is not a broadcast or automated message.. your session is handled by a dedicated support coordinator familiar with the affected
environment.In your Tox session, you will receive:- Secure recovery instructions and validation tools  - A tailored decryption utility for your systems  -
Structured walkthrough of file restoration  - Written disengagement confirmation upon completion  - An overview of observed vulnerabilities for internal
reviewThis is a professional process, designed for completion.. not escalation.═══════════════════════════════════════→ Begin the Session1. Download a Tox
client from https://tox.chat (e.g. qTox or uTox)2. Launch your client and add the following Tox ID:   Tox ID:
[redacted]. Once added, send your assigned Case ID as your first message:   Case ID:
[redacted]Further instructions will be provided once verification is complete.Initial contact does not require commitment. Our goal is
to demonstrate recoverability, answer your questions, and provide guidance toward resolution.═══════════════════════════════════════→ Technical Conduct
GuidelinesTo ensure optimal restoration, we advise:- Do not rename or alter encrypted files.    The recovery software depends on extension-based mapping for
accurate processing.- Avoid using third-party decryptors or system cleaners.    These may damage encrypted headers or corrupt metadata, making restoration
incomplete or impossible.- Do not reimage systems unless explicitly instructed.    Many systems can be restored in-place using verified, offline-capable
tools we provide.- You may duplicate encrypted files for backup or analysis.    However, do not modify the duplicates, as this may break file mapping
integrity.═══════════════════════════════════════→ Timeframe for Private ResolutionTo avoid escalation and ensure a quiet, direct resolution, we reserve your
case as private for the next three (3) working days.If no communication is initiated during this window, your organization may be listed on the ShinySp1d3r
public blog:    http://sh1nysp1[redacted]onionThis listing includes only your company name and incident time till full
disclosure and may include redacted data samples.. not sensitive data. It can be withdrawn once resolution is achieved.═══════════════════════════════════════→
Advisory on Legal or Third-Party InvolvementYou are free to involve any party you choose — legal, government, or external advisory.However, doing so often
increases noise, delays resolution, and limits your ability to manage the event discreetly. This is not a courtroom matter; it is a containment and
restoration scenario.Consider this comparison: hiring a private lawyer to dispute a parking fine may add more stress, cost, and paperwork than simply
resolving the issue directly. The same applies here.You want your systems restored. So do we.═══════════════════════════════════════→ Final Notes on Conduct
and SupportWe recognize this is an unusual and stressful situation. Our policy is to maintain professionalism, confidentiality, and non-escalation
throughout.Your assigned coordinator is available exclusively via the secure Tox session with only the mentioned Tox ID.
```

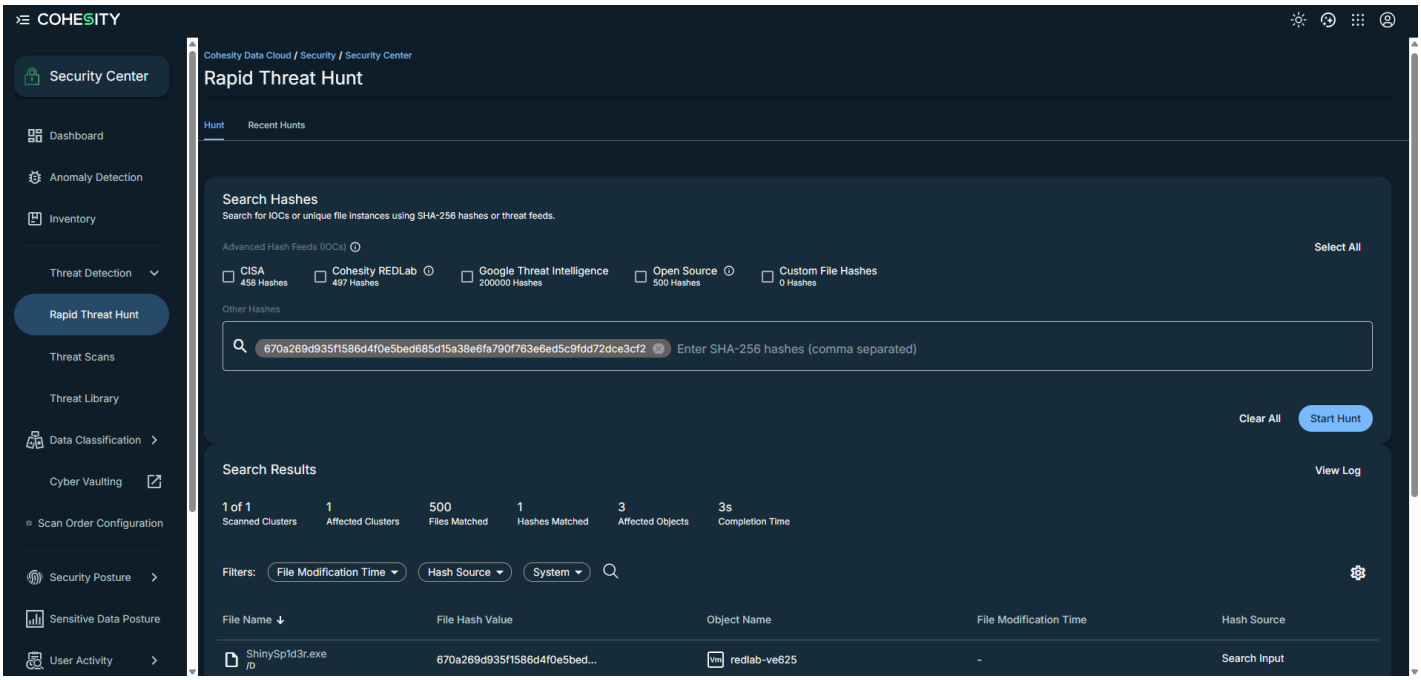
Protection & Detection Outcomes

After the attack, the DataProtect VMware backup operations remained unaffected. Despite the ransomware attack, backups were executed successfully. Also, in the case of NetBackup an Image Entropy anomaly that detected unusual deviation in VMware backup job attributes 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 ShinySp1d3r 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. DataProtect and NetBackup VMware based backup and recovery was successful.

Summary

- For all the ransomware strains described earlier, VMware protection runs for the DataProtect 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.

- Similarly in case of NetBackup an Image Entropy anomaly that detected unusual deviation in VMware backup job attributes was generated for all the above mentioned strains post attack. 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