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

Strain Details	SHA-256 Hash (VirusTotal)
Name: Black TENGU Family: Babuk-derived (Black TENGU) Ransomware	fce73d80e9dd23d2156476af59565d609cb70de35500a65f6085268272fc28db
Name: Chip Family: MedusaLocker Ransomware Family	4121140cb90d1022a3b42305b833e04a46e7ab28a0d9dadcc43e2c922c5bf1f0
Name: NBLock Family: NBLock Ransomware	cb098ef829114f0369097e4a73b5f8788efe6f11ad16e0dbe39accca4fb2b628
Name: Aur0ra Family: Aur0ra Ransomware	81ca5fc6b55accdbc44266d66bd72c7c4152a75b215593adc433d51250054333

Black TENGU Ransomware

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

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

Malware impact post execution

Black TENGU is a 32-bit PE32 ransomware payload built on a leaked Babuk ransomware codebase, confirmed by the distinctive embedded mutex string “DoYouWantToHaveSexWithCuongDong” carried over from Babuk's original builder. After profiling the host and enumerating running services and processes for anti-VM checks, it strips read-only attributes from hundreds of files (506 observed) before encrypting them and appending a “.TENGU” extension, while separately overwriting and mass-deleting a large share of touched files – a more destructive, wiper-adjacent pattern than pure encryption alone. It disables shadow copies via vssadmin.exe delete shadows /all /quiet and drops its ransom note, “_README_TENGU.txt”, throughout the file system. The note claims data theft alongside encryption and directs victims to a .onion leak-site/negotiation chat or two named email addresses, quoting a unique victim ID and a promise to delete stolen data upon payment.

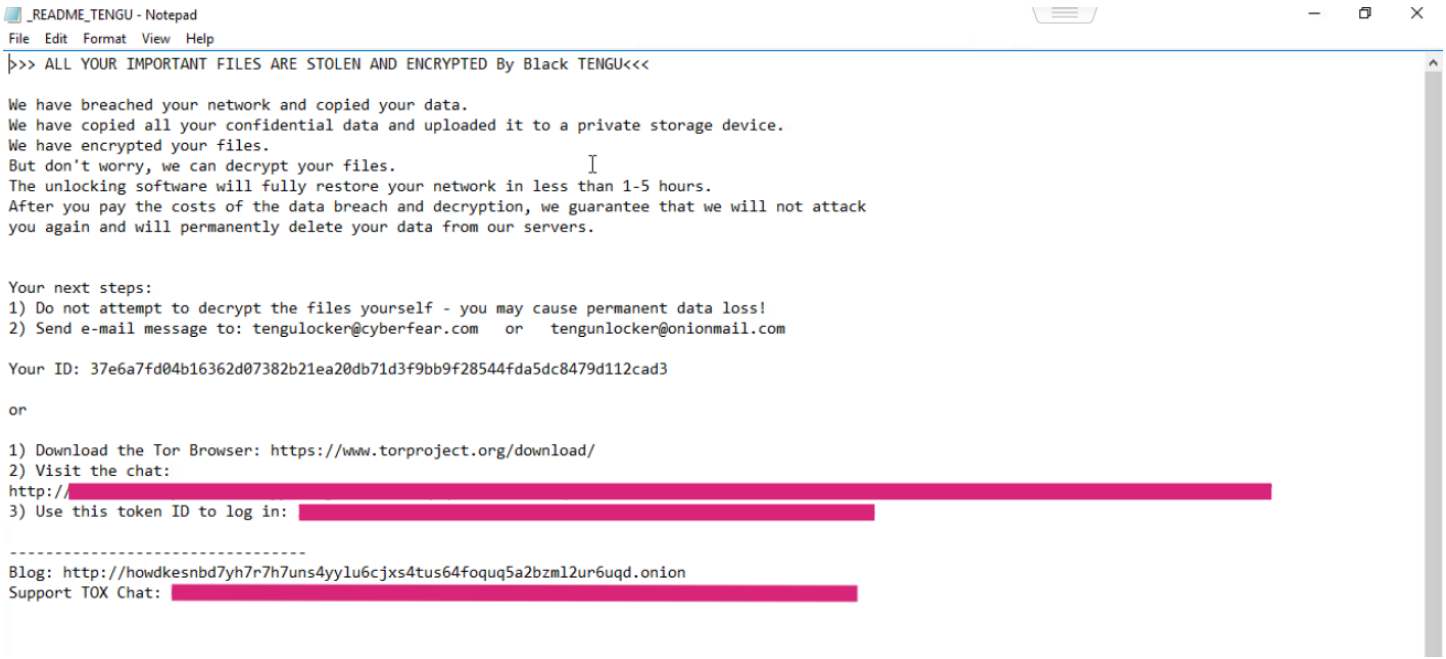


Image: Ransom note dropped as _README_TENGU.txt.

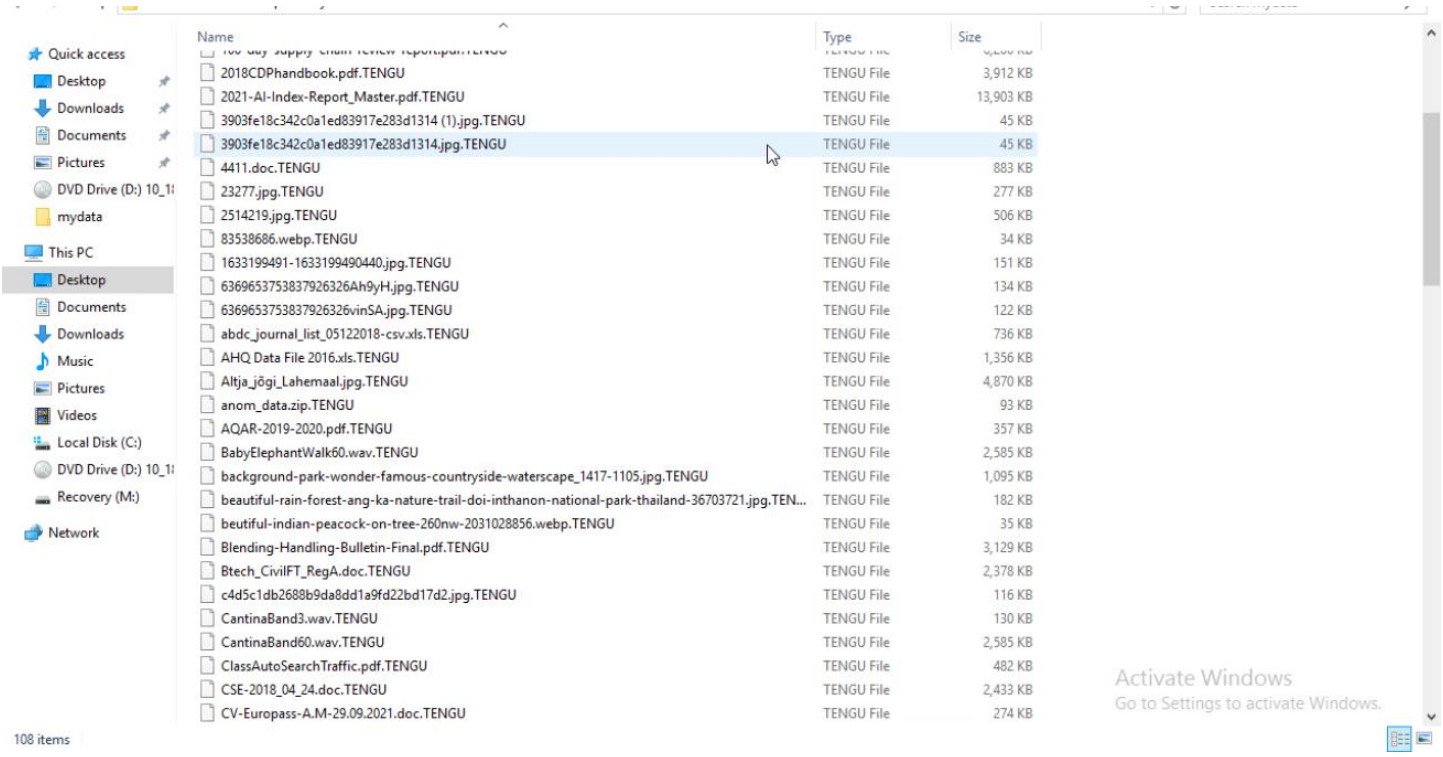
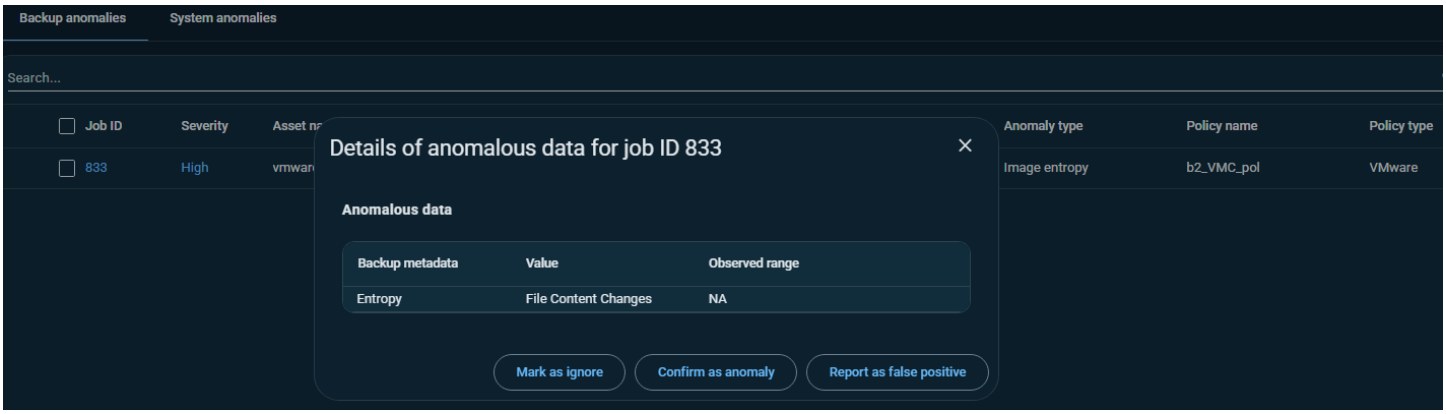


Image: Post-attack file listing showing the .TENGU extension appended to encrypted files.

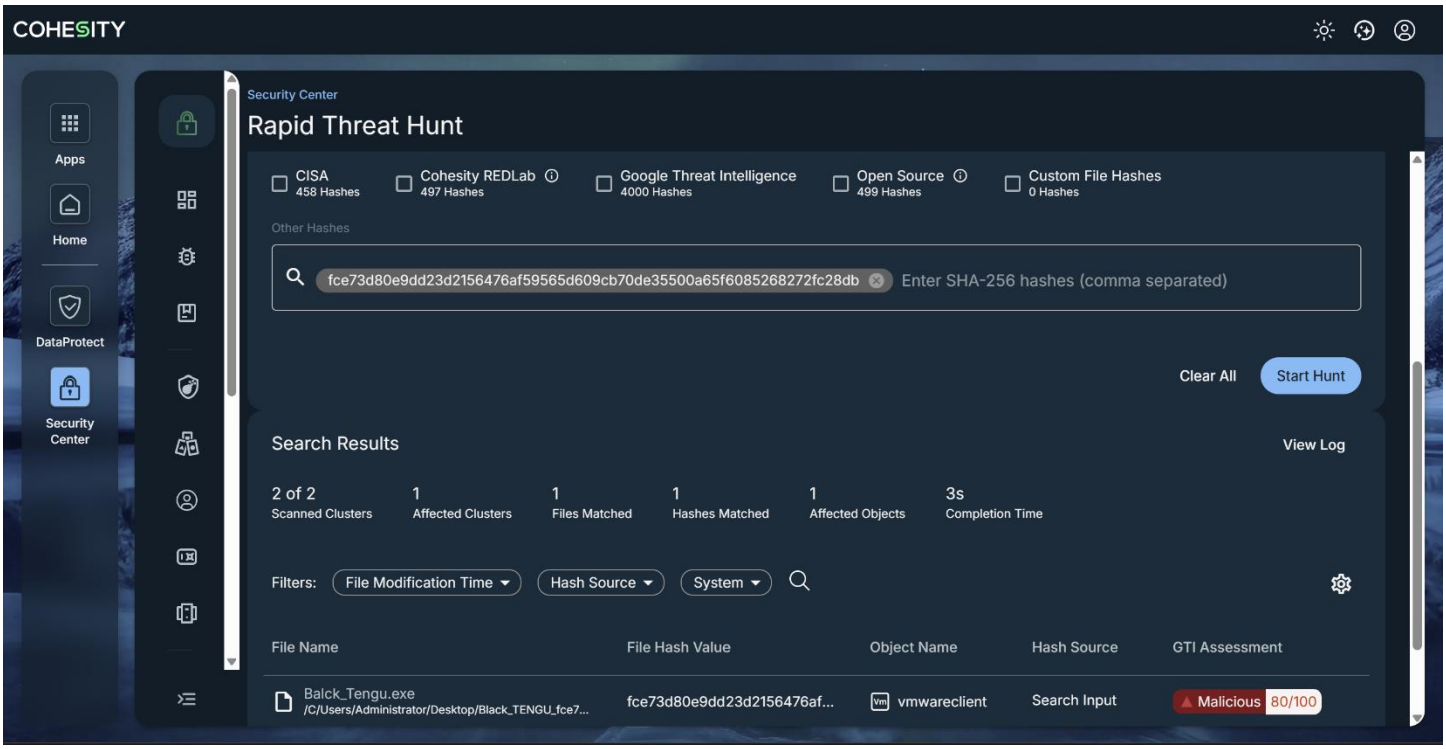
Protection & Detection Outcomes

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.



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 Black TENGU 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.

Chip Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Shared Modules	T1129	Execution
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Access Token Manipulation	T1134	Privilege Escalation, Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Hide Artifacts	T1564	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
Input Capture	T1056	Credential Access, Collection
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Deobfuscate/Decode Files or Information	T1140	Defense Evasion
Application Window Discovery	T1010	Discovery
Query Registry	T1012	Discovery
System Location Discovery	T1614	Discovery

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

Malware impact post execution

Chip is a 64-bit Windows executable flagged by the majority of AV engines as a MedusaLocker-family ransomware variant, consistent with the classic MedusaLocker playbook. Sandbox analysis confirms it loads additional shared modules at runtime, establishes autostart persistence via the registry, and manipulates access tokens to elevate privileges while evading defenses through obfuscated/packed code and virtualization and sandbox checks. It also exhibits input-capture behavior alongside broad system and file/directory discovery, consistent with reconnaissance of the host prior to encryption. It masquerades a dropped payload under a generic system-process-style filename inside C:\Windows, and leverages the Windows Restart Manager API (RstrtMgr.dll) to force-close applications holding target files open so encryption is not blocked by file locks. Encrypted files are renamed with a distinctive ".chip1" extension, the desktop wallpaper is overwritten via a registry-based defacement to display the attacker's contact address, and an HTML ransom note is dropped threatening to publish exfiltrated data and raise the price if the victim does not respond within 72 hours.

Image: Desktop wallpaper defaced with attacker contact email post-attack.

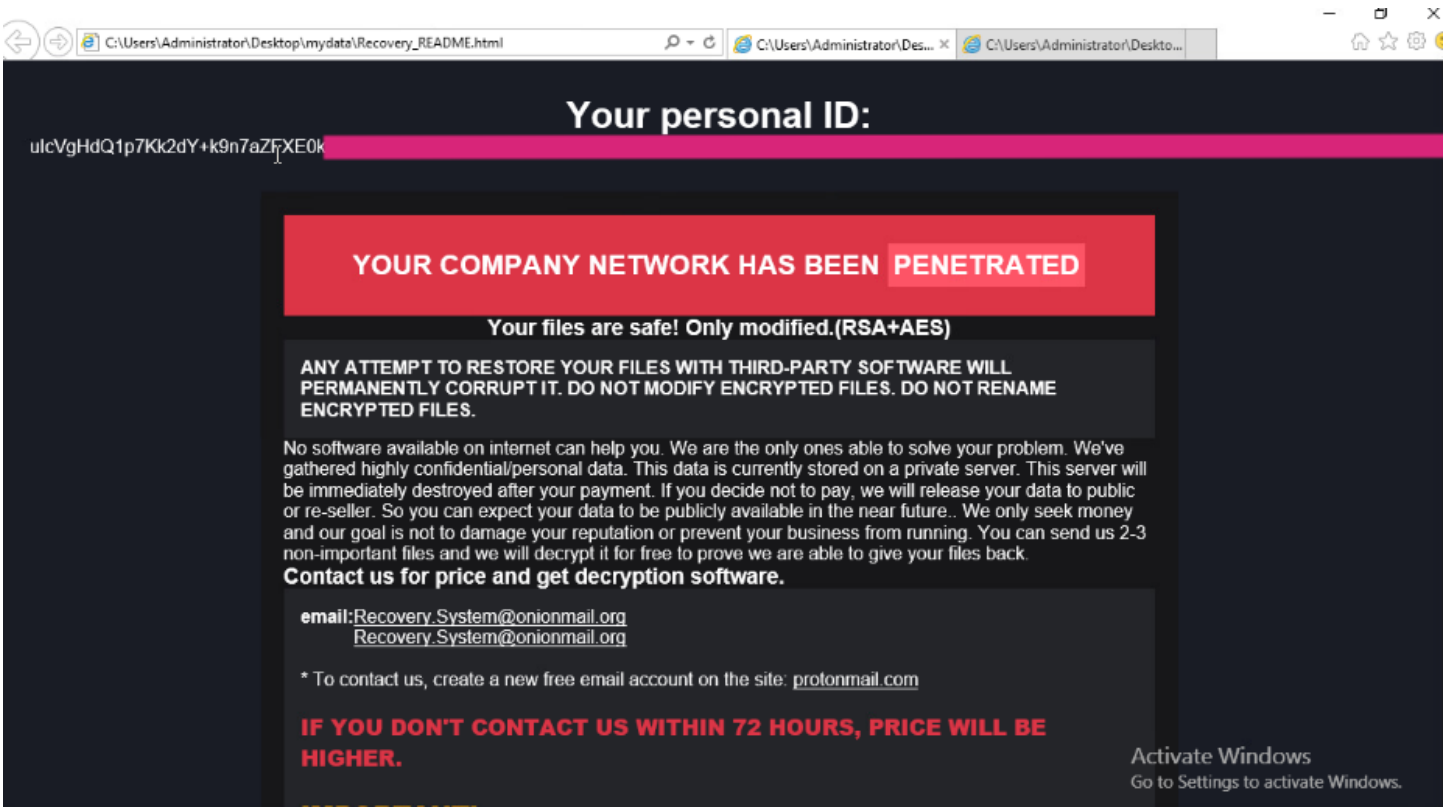
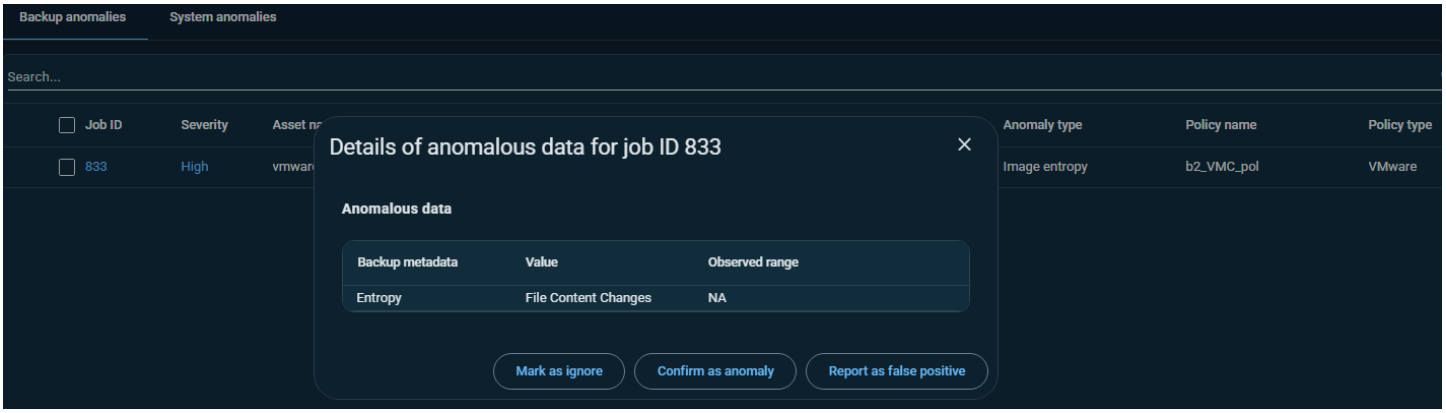


Image: HTML ransom note (Recovery_README.html) dropped post-attack.

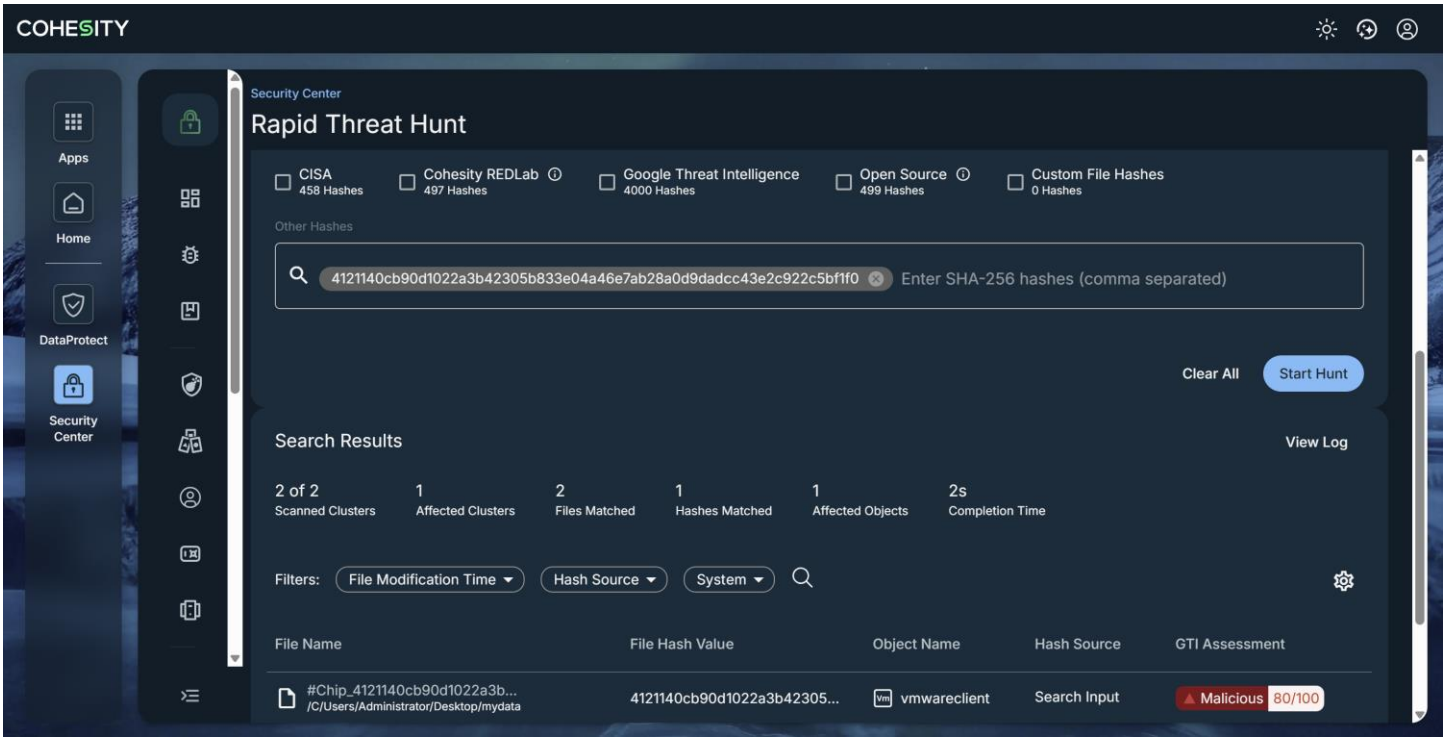
Protection & Detection Outcomes

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.



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 Chip 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.

NBLock Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Windows Management Instrumentation	T1047	Execution
Shared Modules	T1129	Execution
Native API	T1106	Execution
Command and Scripting Interpreter	T1059	Execution
Hijack Execution Flow	T1574	Persistence, Privilege Escalation, Defense Evasion
Process Injection	T1055	Defense Evasion, Privilege Escalation
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Hide Artifacts	T1564	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Masquerading	T1036	Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Software Packing	T1027.002	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
System Owner/User Discovery	T1033	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Application Layer Protocol	T1071	Command and Control
Data Encrypted for Impact	T1486	Impact
Data Destruction	T1485	Impact

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

Malware impact post execution

NBLock is a 32-bit .NET/Mono assembly (roughly 107KB) whose core file-encryption routine is implemented in an async method internally named RunNBLock. Before encrypting, it profiles the host via system and user discovery, abuses Windows Management Instrumentation and the Native API to execute payloads, and evades analysis through packed and obfuscated code, hidden windows, and virtualization/sandbox checks, while process injection and execution-flow hijacking are used to escalate privileges and persist. It disables recovery via vssadmin.exe delete shadows /all /quiet, then encrypts files with AES-256, appending a distinctive ".NBLock" extension and instructing victims not to delete or modify a locally dropped "key.bin" file, described in the note as the only recovery tool. The desktop wallpaper is overwritten with a black screen reading "YOUR FILES ARE ENCRYPTED — READ README_NBLOCK.TXT FOR INSTRUCTIONS", and the matching ransom note (README_NBLOCK.txt) directs victims to install the Tor Browser and visit a negotiation .onion address for a decryptor.

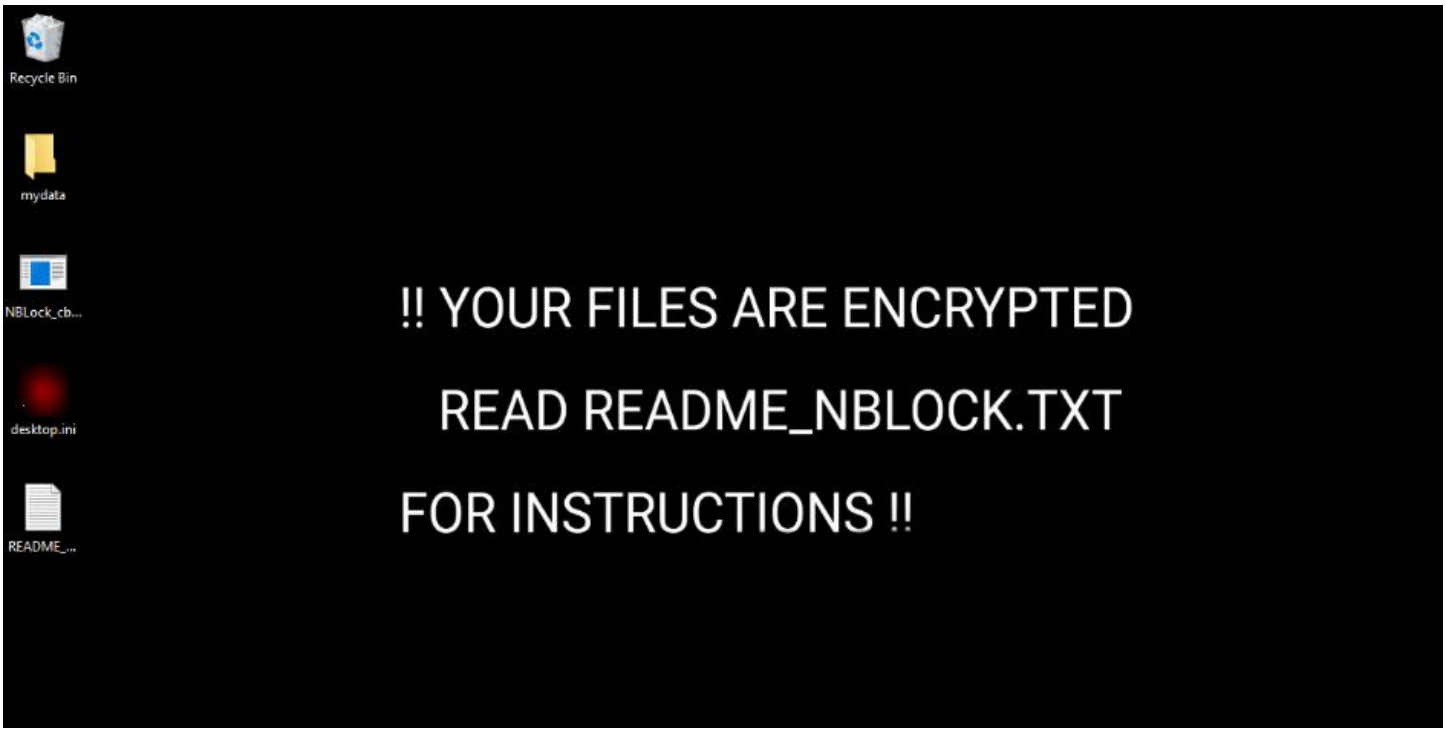


Image: Desktop wallpaper overwritten with an encryption notice post-attack.

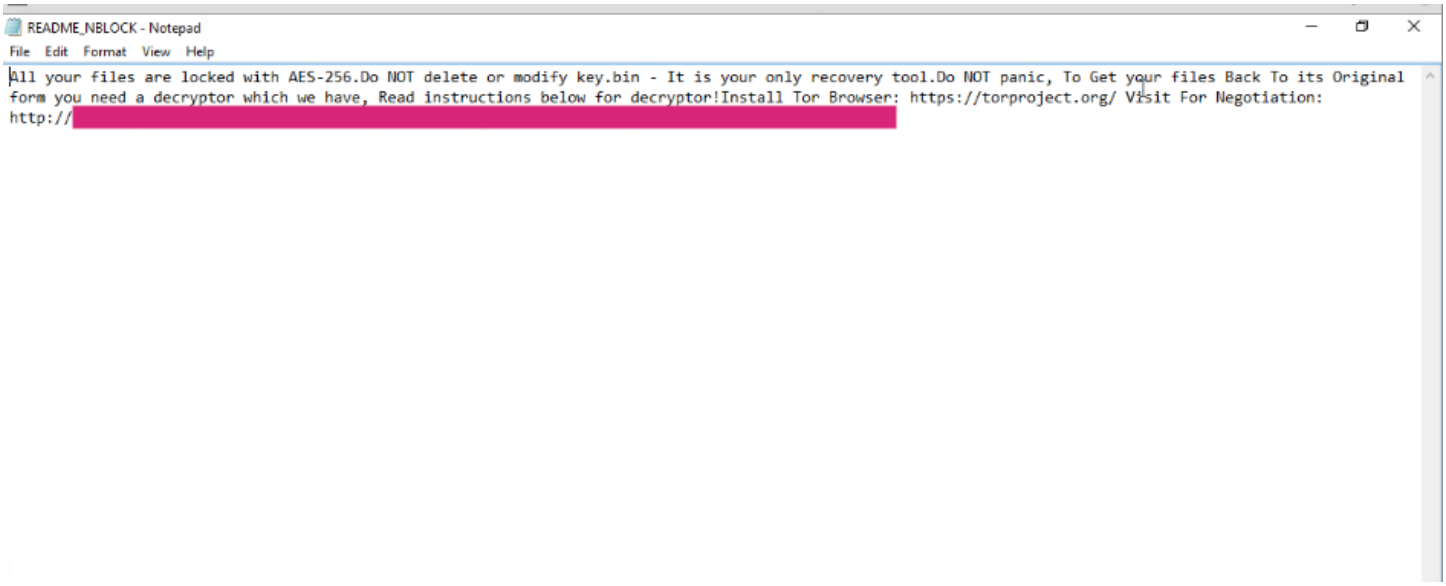
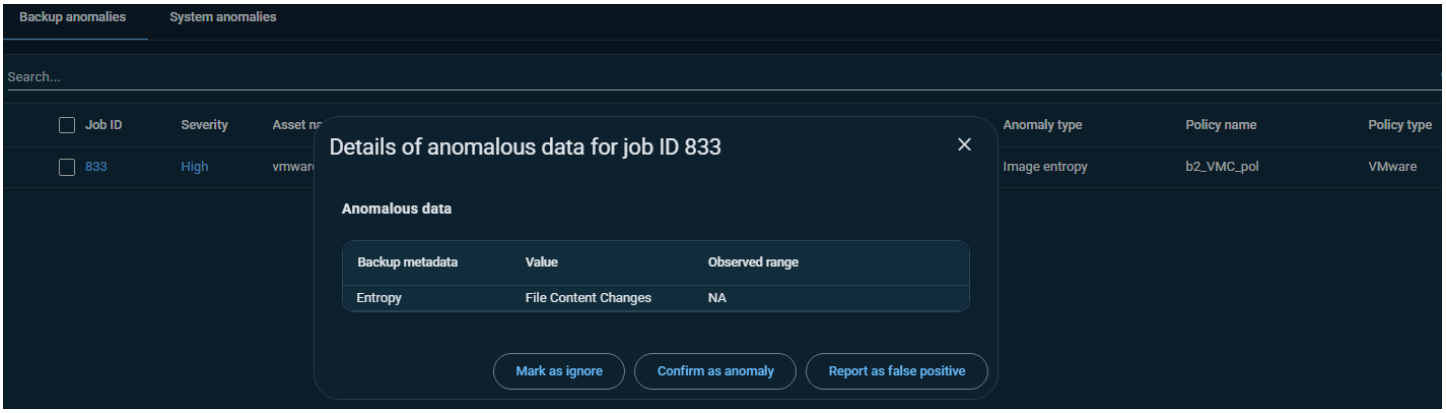


Image: Ransom note dropped as README_NBLOCK.txt.

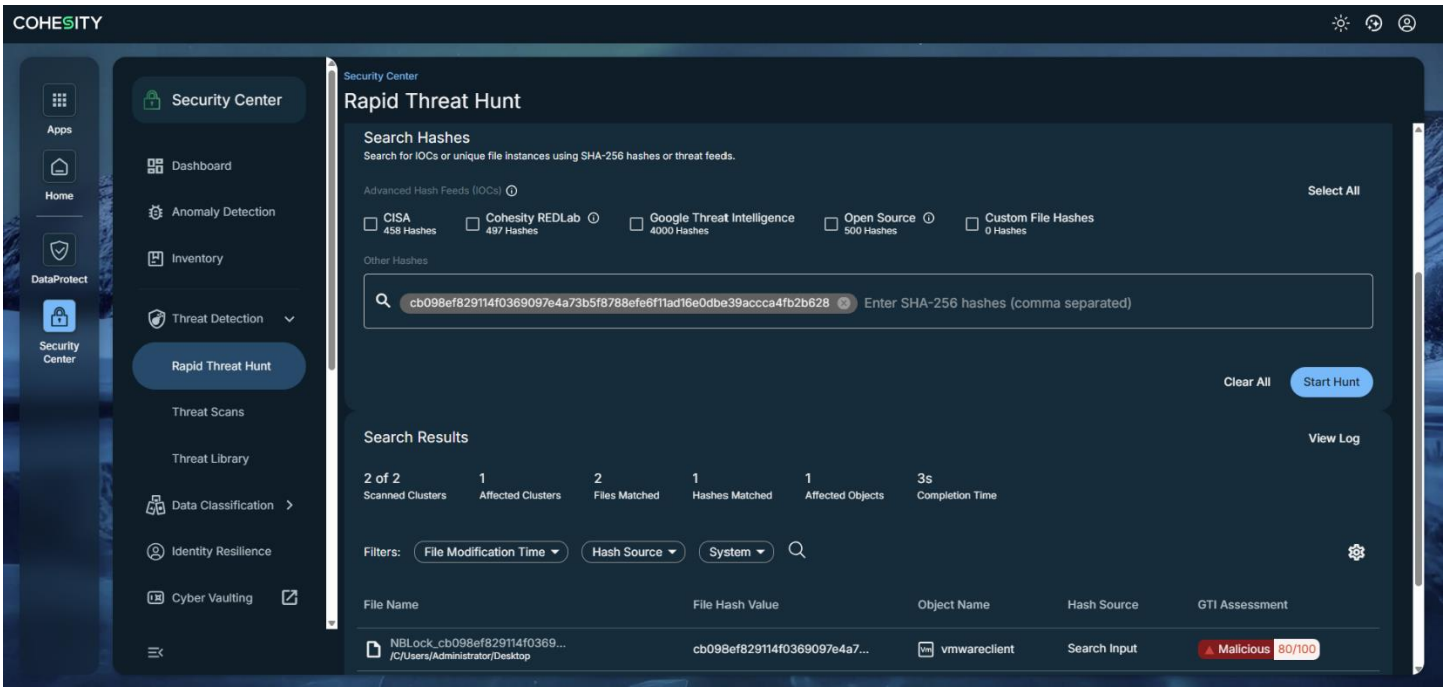
Protection & Detection Outcomes

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.



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 NBLock 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.

Aur0ra Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Process Injection	T1055	Defense Evasion, Privilege Escalation
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Hide Artifacts	T1564	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Masquerading	T1036	Defense Evasion
Timestomp	T1070.006	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Software Packing	T1027.002	Defense Evasion
System Owner/User Discovery	T1033	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Process Discovery	T1057	Discovery
Query Registry	T1012	Discovery
Application Layer Protocol	T1071	Command and Control
Data Encrypted for Impact	T1486	Impact
Data Destruction	T1485	Impact

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

Malware impact post execution

Aur0ra is a native, non-.NET PE32+ (x86-64) ransomware binary that pairs conventional data-destruction tradecraft with in-place file encryption: rather than appending a distinctive extension, it re-encrypts documents and media while preserving their original filenames and extensions, complicating extension-based detection heuristics. It leverages the Windows CryptoAPI (CryptAcquireContext/CryptGenRandom) to seed encryption key material, hollows a legitimate svchost.exe process via a suspended-process and remote-thread-resume technique to blend in, and profiles the host (hardware ID, volume serial number, running services, FIPS policy) before detonating. Recovery is systematically dismantled: vssadmin delete shadows /all /quiet, wmic shadowcopy delete, a resized shadow-storage cap (401MB), and a disabled Windows System Restore scheduled task. It then drops a double-extortion ransom note, “!!!README!!!DO_NOT_DELETE.txt”, across 61 directories, directing victims to a Tor .onion negotiation portal and a supplied access key.

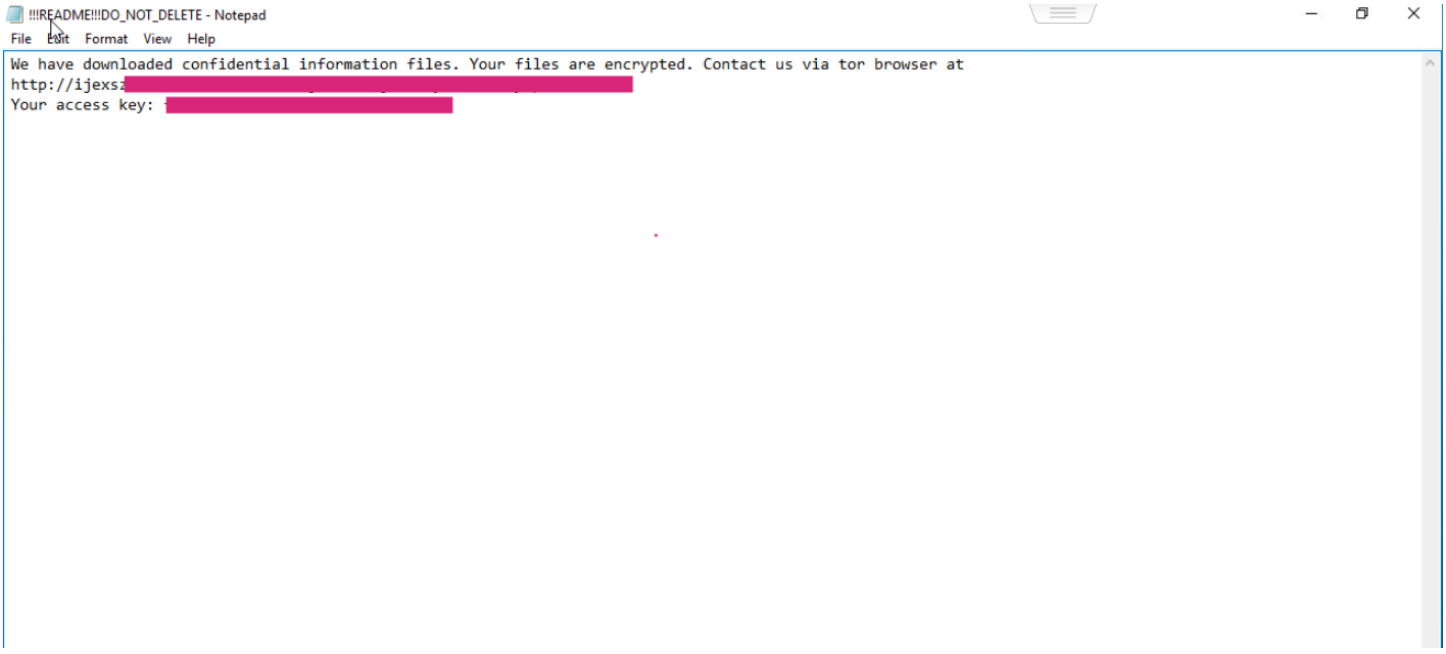


Image: Ransom note dropped as !!!README!!!DO_NOT_DELETE.txt.

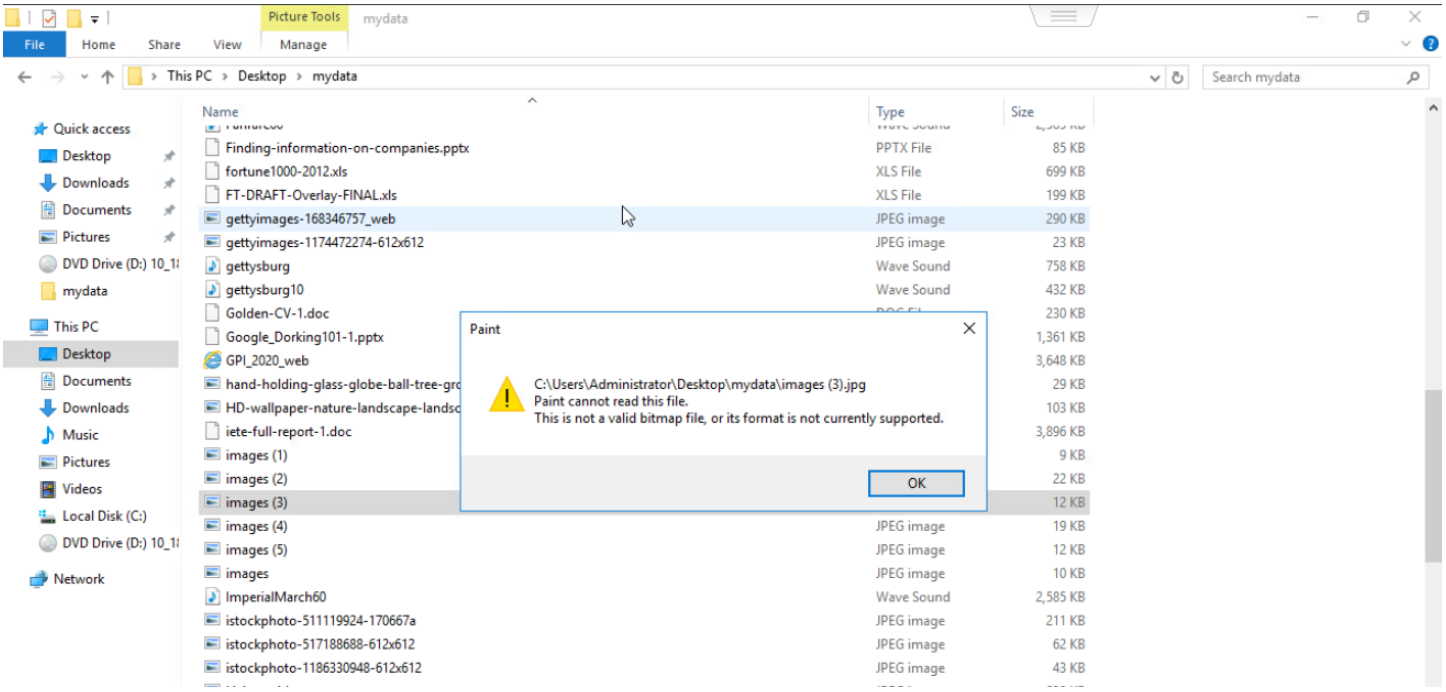


Image: Encrypted JPEG image file rendered unreadable by imaging software post-attack.

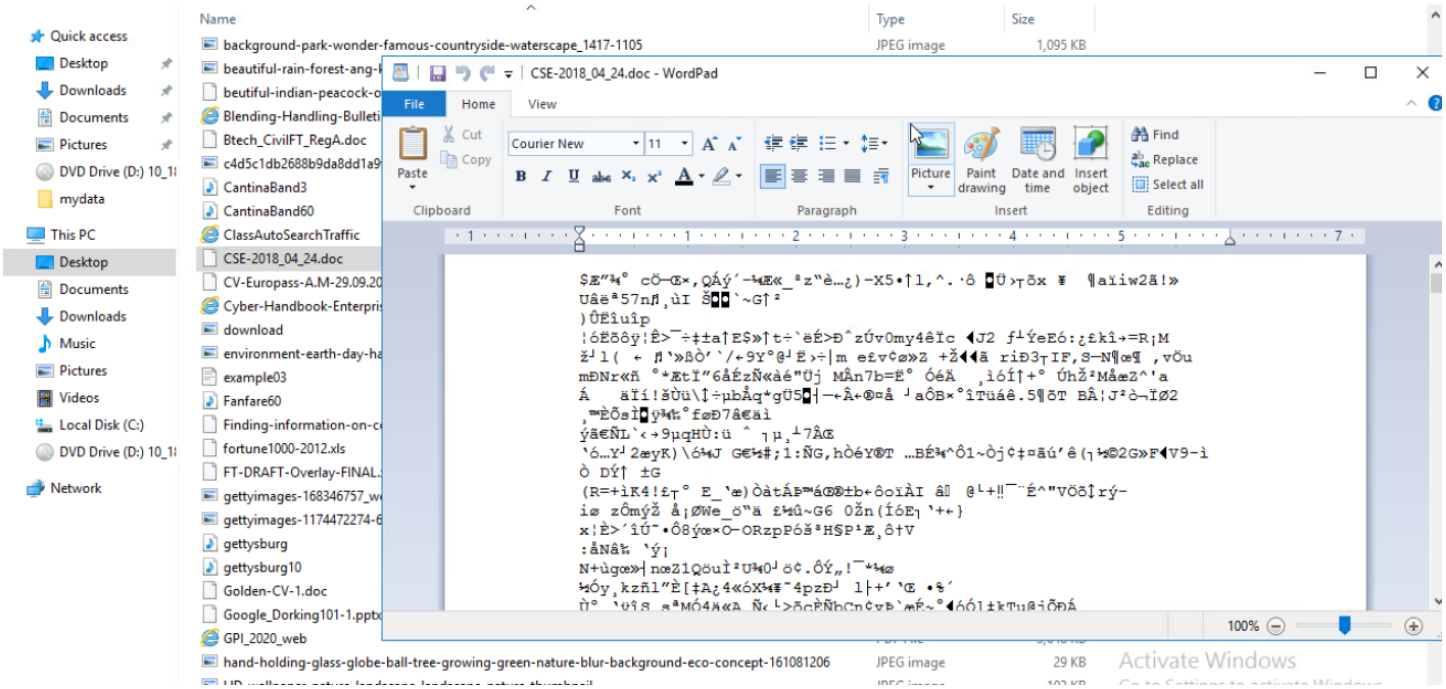


Image: Encrypted Word document rendered unreadable in WordPad post-attack.

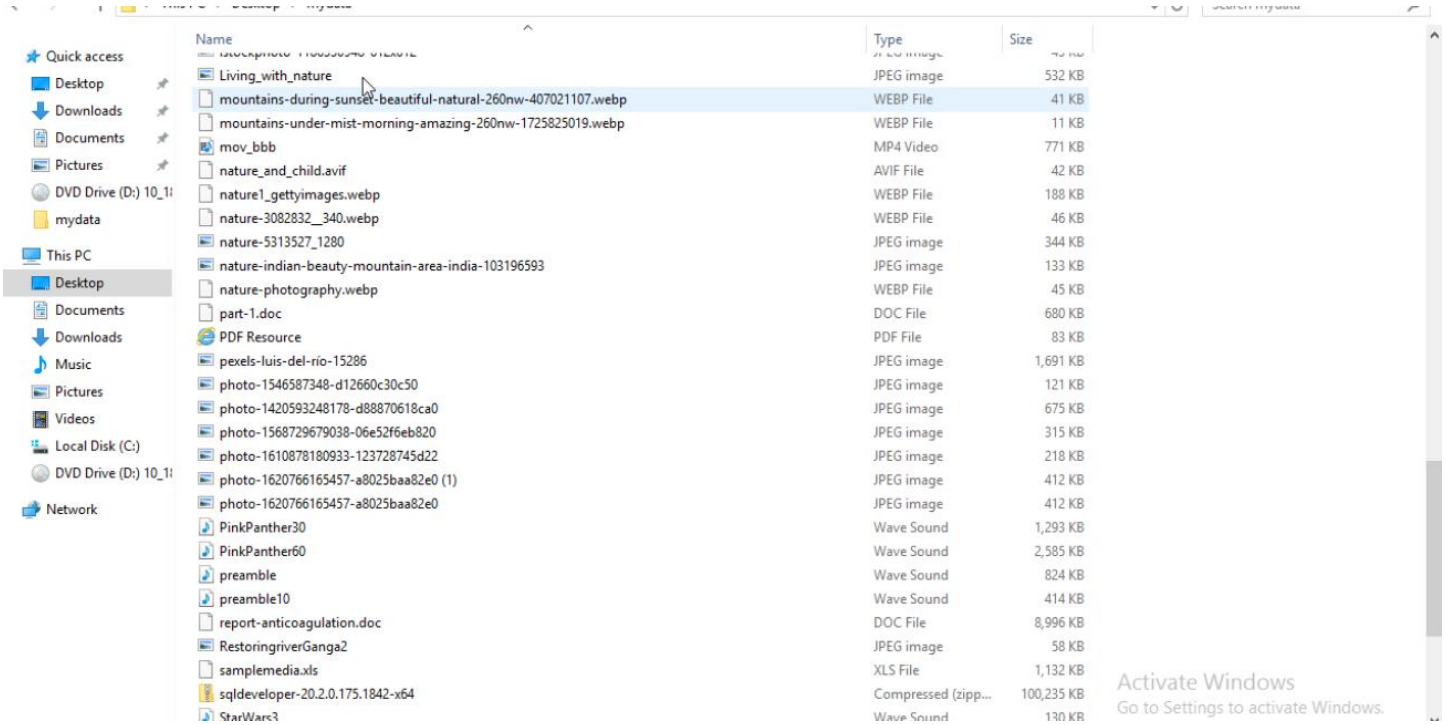
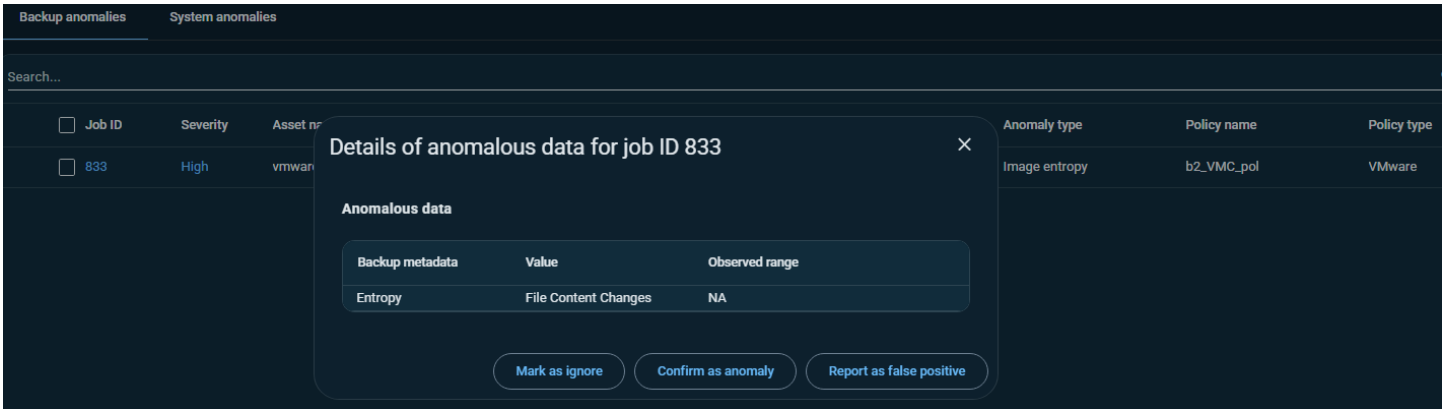


Image: Post-attack file listing showing original filenames and extensions preserved despite encryption.

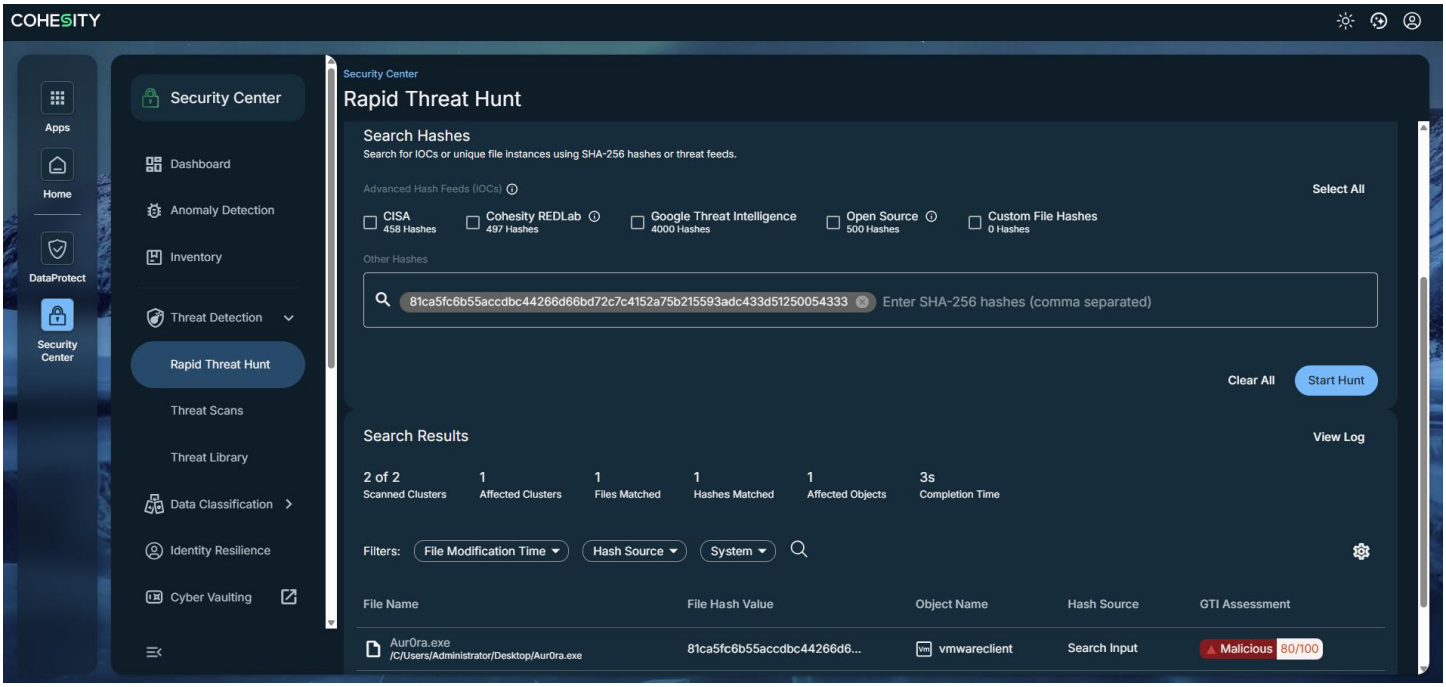
Protection & Detection Outcomes

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.



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 Aur0ra 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

- Both DataProtect and NetBackup achieved successful VMware backup and recovery across all four ransomware strains tested this month - Black TENGU, Chip, NBLock and Aur0ra, 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 proactively 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