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 analysing 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: LSD Family: LSD Team	9b6160bb11b8981741a2ee52301bbf157e2aa9aab1b33d4e4552b6a4146729ec
Name: NBLock Black Family: NBLock Group	59dd29982f9644046b726452978de2dbed11d12c4c5a7eb22e4ad52d7951c16d
Name: Witch Family: Witch Ransomware	6fd647f5f80e2b0861e1abdc05a0d748b28de6c1ca3030c2855b9388cad4cf8c
Name: Gunra Family: ContiV2 Family	854e5f77f788bbbe6e224195e115c749172cd12302afca370d4f9e3d53d005fd

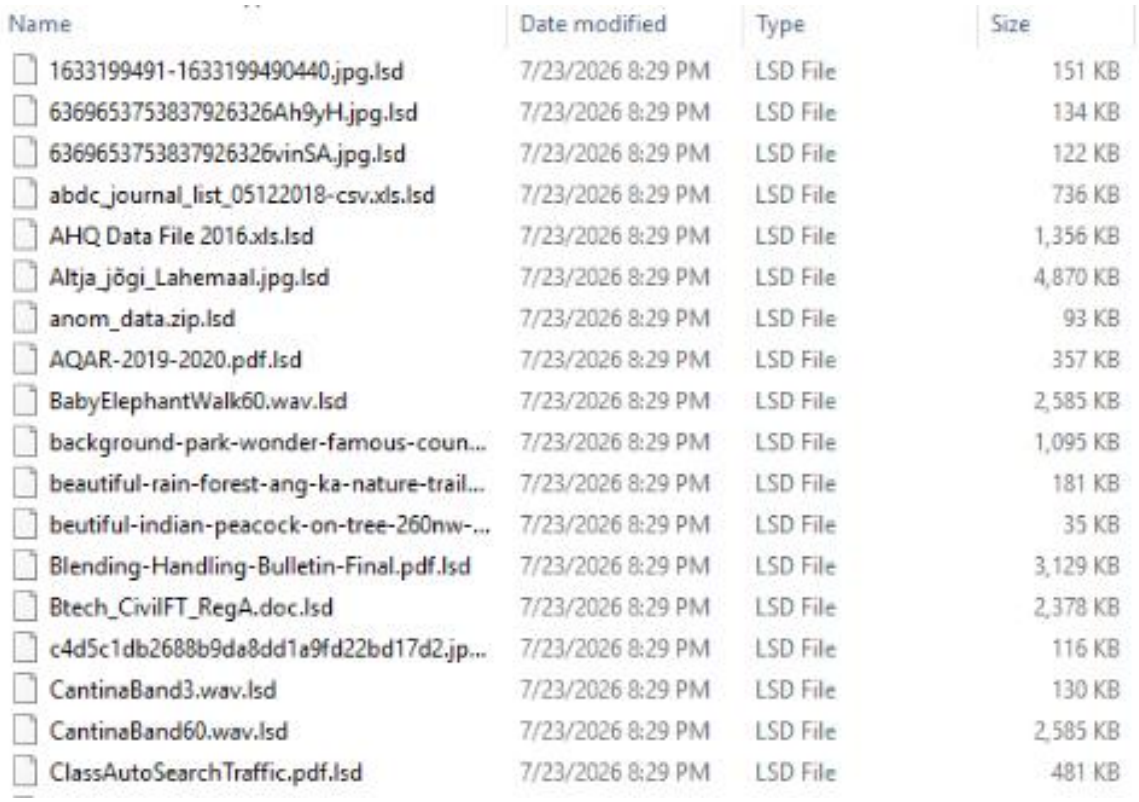
LSD Ransomware

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
Hijack Execution Flow	T1574	Defense Evasion, Privilege Escalation, Persistence
Indicator Removal	T1070	Defense Evasion
Timestomp	T1070.006	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Command and Scripting Interpreter	T1059	Execution
Shared Modules	T1129	Execution
Application Layer Protocol	T1071	Command and Control
Data Staged	T1074	Collection
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

LSD is a compact 32-bit Windows .NET ransomware payload (approximately 33 KB) attributed to the "LSD Team". It profiles the host for virtualisation and sandboxing. It applies anti-debugging and delayed execution. It also reads locale and hardware identifiers consistent with geofencing and victim keying. It then loads via a heavily obfuscated, shellcode-staging loader that hijacks execution flow from a hidden window. On impact, LSD encrypts victim files with a ".lsd" extension (467 files during detonation), alongside mass file deletion, overwriting, Recycle Bin manipulation and cleared event logs. Its most severe impact, however, was to the boot chain itself. The ransom note claims the MBR, VBR, SSD controller and UEFI/BIOS firmware have been compromised. This was borne out post-execution: the Start button and taskbar were removed. After reboot the guest failed to boot entirely, with the Windows Boot Manager, EFI virtual disk and virtual SATA CDROM all failing and the system falling through to a PXE network boot. LSD renders the host unbootable at the firmware level, making this one of the most destructive strains observed this month. Discord infrastructure callbacks were observed, consistent with command, control and exfiltration use.



Name	Date modified	Type	Size
1633199491-1633199490440.jpg.lsd	7/23/2026 8:29 PM	LSD File	151 KB
636965375383792632 6Ah9yH.jpg.lsd	7/23/2026 8:29 PM	LSD File	134 KB
636965375383792632 6vinSA.jpg.lsd	7/23/2026 8:29 PM	LSD File	122 KB
abdc_journal_list_05122018-csv.xls.lsd	7/23/2026 8:29 PM	LSD File	736 KB
AHQ Data File 2016.xls.lsd	7/23/2026 8:29 PM	LSD File	1,356 KB
Altja_jõgi_Lahemaal.jpg.lsd	7/23/2026 8:29 PM	LSD File	4,870 KB
anom_data.zip.lsd	7/23/2026 8:29 PM	LSD File	93 KB
AQAR-2019-2020.pdf.lsd	7/23/2026 8:29 PM	LSD File	357 KB
BabyElephantWalk60.wav.lsd	7/23/2026 8:29 PM	LSD File	2,585 KB
background-park-wonder-famous-coun...	7/23/2026 8:29 PM	LSD File	1,095 KB
beautiful-rain-forest-ang-ka-nature-trail...	7/23/2026 8:29 PM	LSD File	181 KB
beutiful-indian-peacock-on-tree-260nw-...	7/23/2026 8:29 PM	LSD File	35 KB
Blending-Handling-Bulletin-Final.pdf.lsd	7/23/2026 8:29 PM	LSD File	3,129 KB
Btech_CivilFT_RegA.doc.lsd	7/23/2026 8:29 PM	LSD File	2,378 KB
c4d5c1db2688b9da8dd1a9fd22bd17d2.jp...	7/23/2026 8:29 PM	LSD File	116 KB
CantinaBand3.wav.lsd	7/23/2026 8:29 PM	LSD File	130 KB
CantinaBand60.wav.lsd	7/23/2026 8:29 PM	LSD File	2,585 KB
ClassAutoSearchTraffic.pdf.lsd	7/23/2026 8:29 PM	LSD File	481 KB

Image: Victim files following detonation, each appended with the ".lsd" extension.

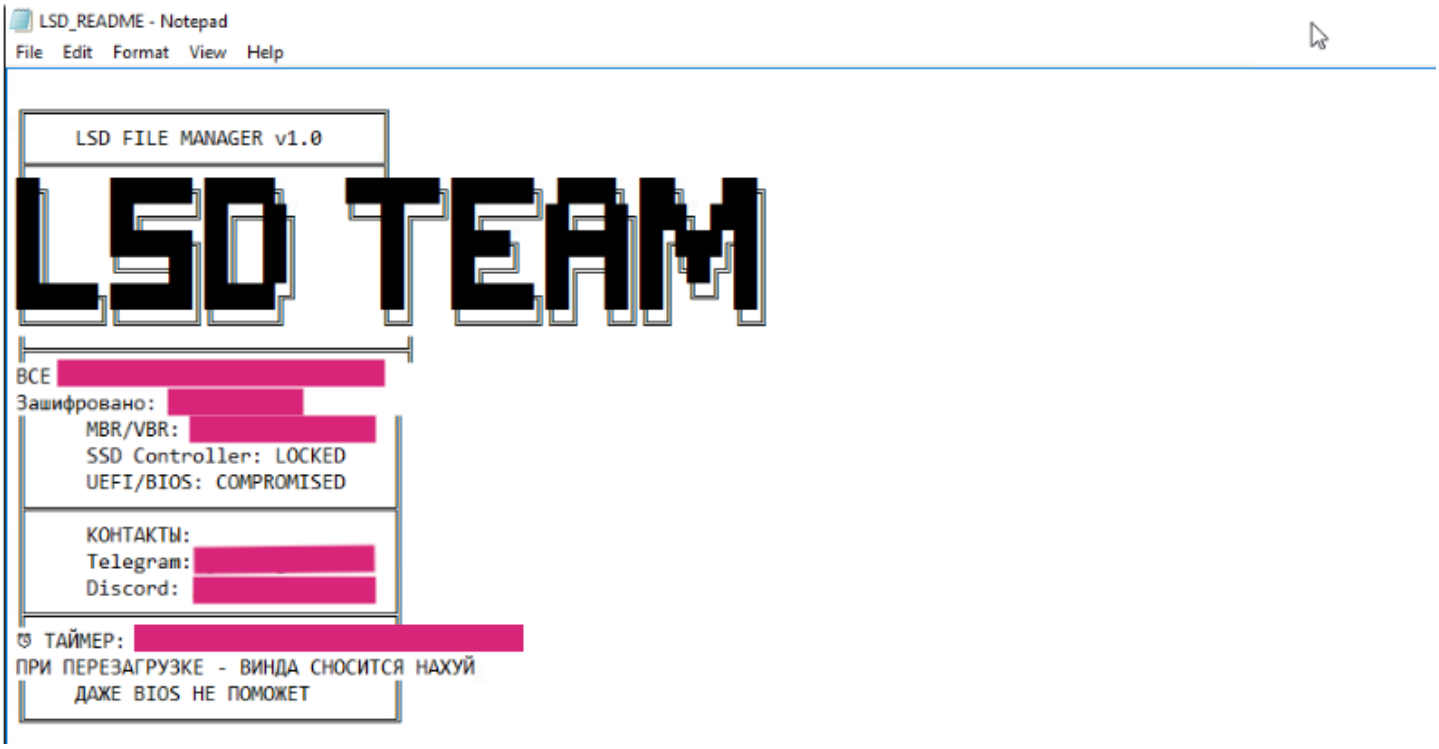


Image: The "LSD_README" ransom note.

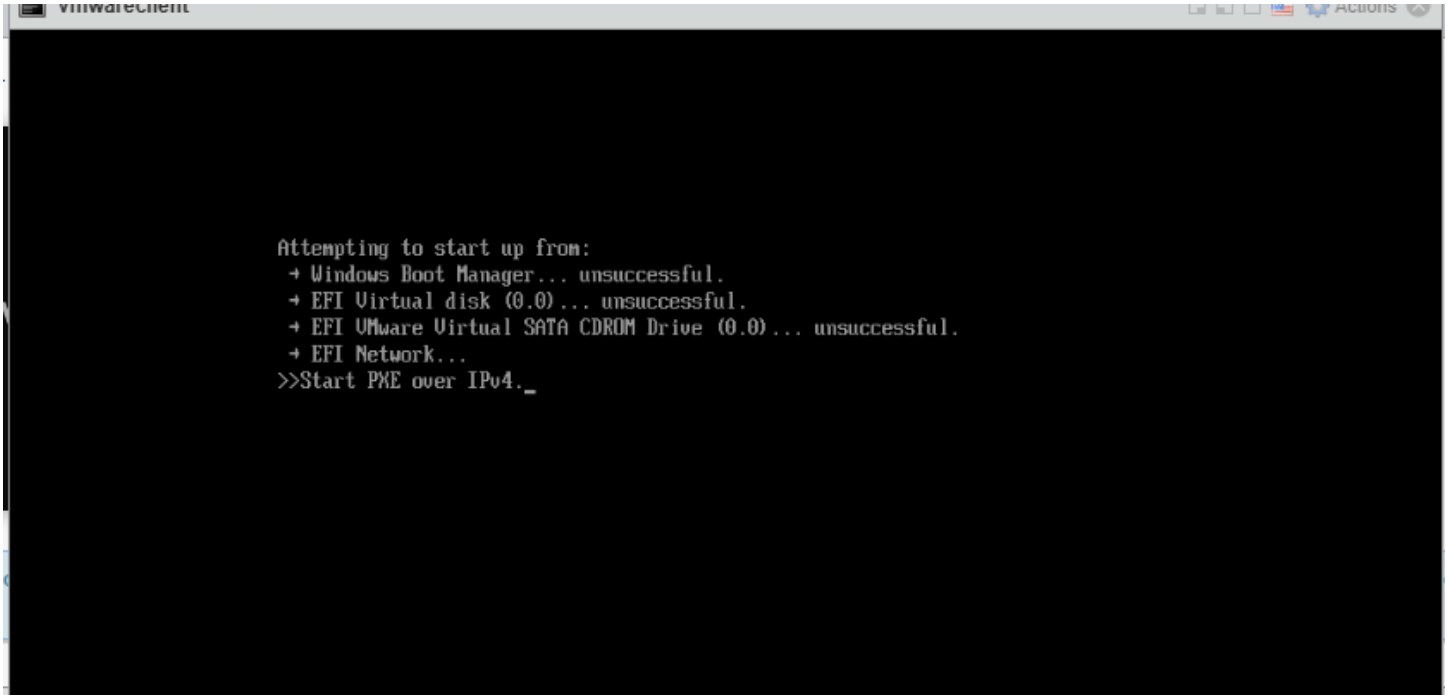
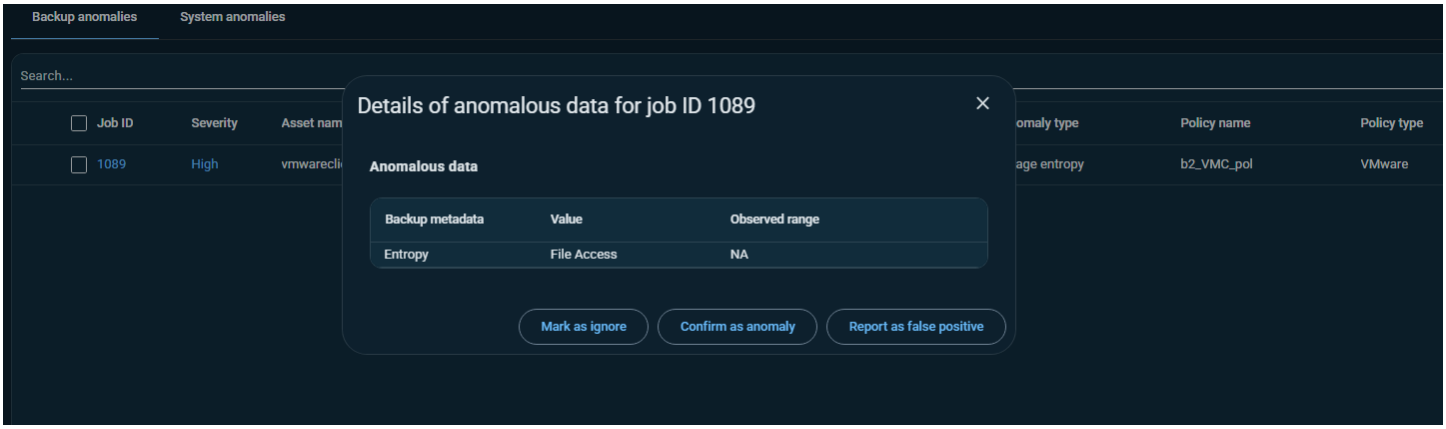


Image: After reboot, the guest fails to start from Windows Boot Manager or the EFI virtual disk and falls through to a PXE network boot.

Image: Firmware boot sequence reporting no bootable media on any configured device.

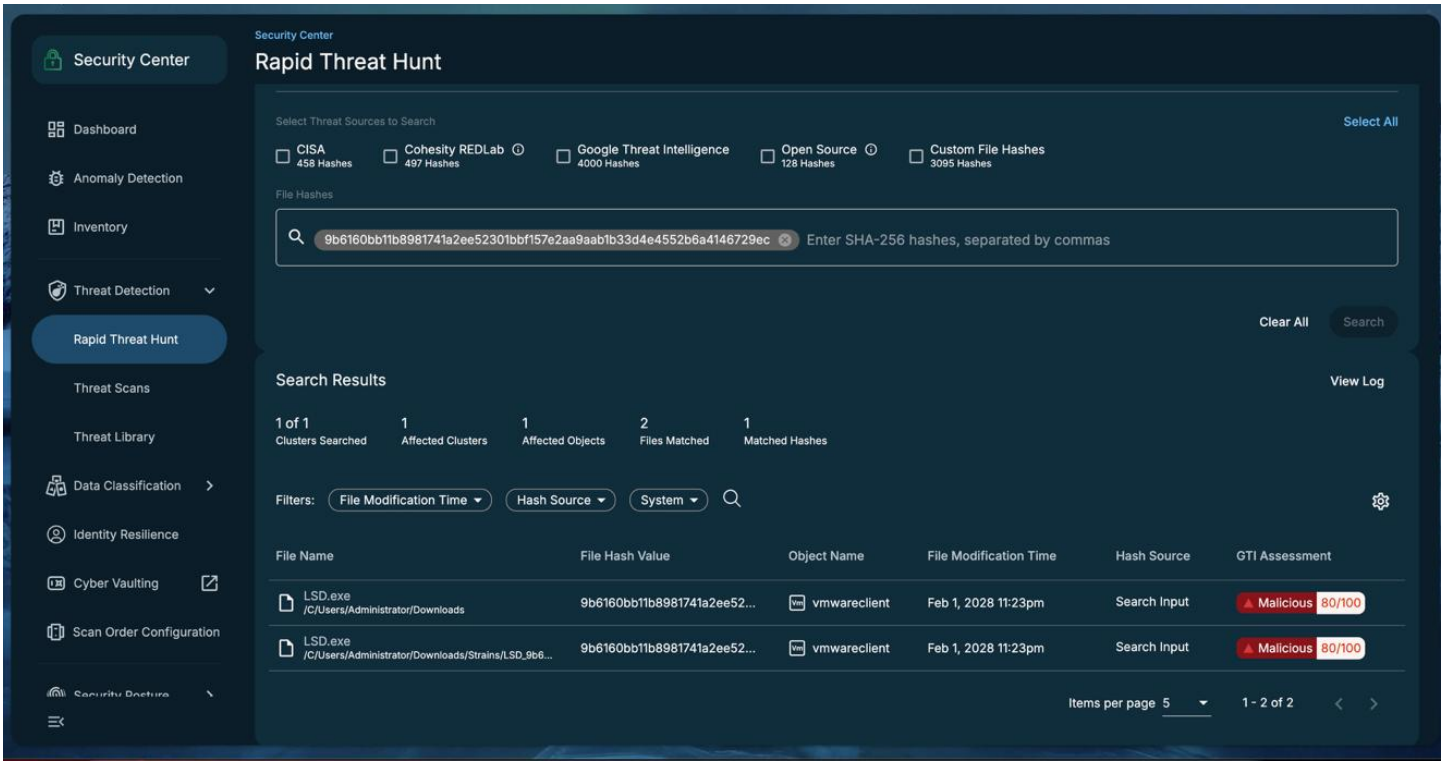
Protection & Detection Outcomes

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 LSD 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 Black Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Inhibit System Recovery	T1490	Impact
Internal Defacement	T1491.001	Impact
Application Layer Protocol	T1071	Command and Control
Native API	T1106	Execution
Indicator Removal	T1070	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Impair Defenses	T1562	Defense Evasion
OS Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
System Information Discovery	T1082	Discovery
Software Discovery	T1518	Discovery
Data from Local System	T1005	Collection
Email Collection	T1114	Collection
Encrypted Channel	T1573	Command and Control
Data Destruction	T1485	Impact

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

Malware impact post execution

NBLock Black is a large 64-bit Windows PE ransomware payload (approximately 12 MB), consistent with a bundled/packed distribution.

On execution, NBLock Black assigns the host a victim identifier, then renames and encrypts victim files with an identifier-derived extension (observed as ".c8209") removing the filename as a recovery aid. Its ransom note, "README_NBLOCK.txt", names the victim ID, and the desktop wallpaper is replaced with a full-screen double-extortion notice claiming data theft and encryption. Local recovery was disrupted: Windows Server Backup reported no available local backup configuration after the attack.

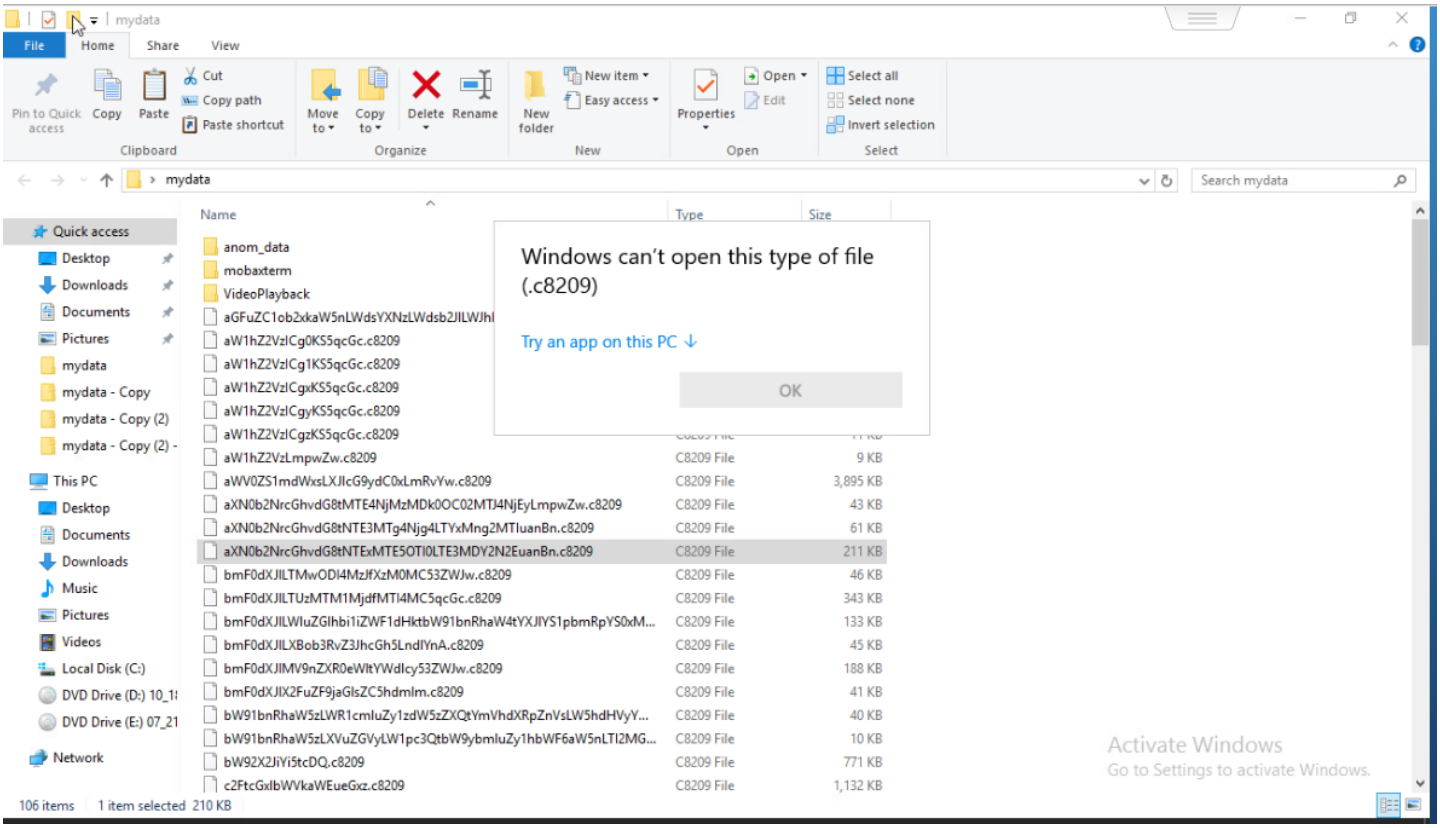


Image: Victim files renamed to opaque encoded strings and appended with the victim-ID derived ".c8209" extension.

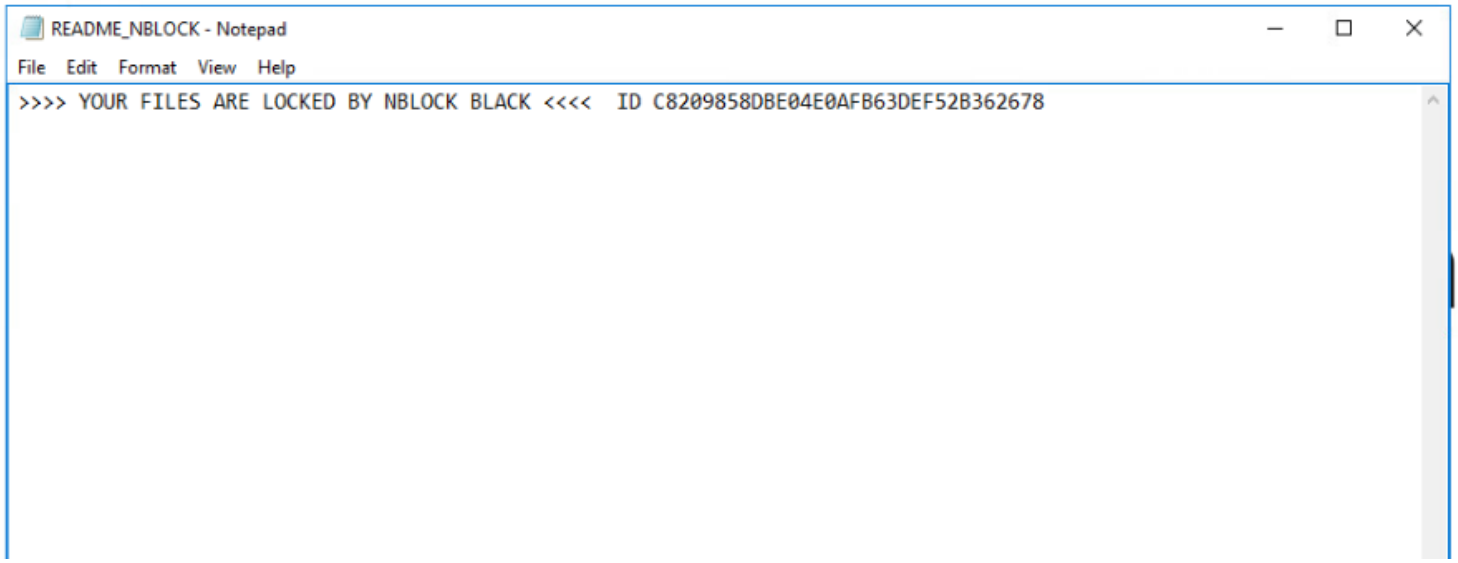


Image: The "README_NBLOCK.txt" ransom note stating that files are locked by NBLock Black, with the victim ID assigned to the host.

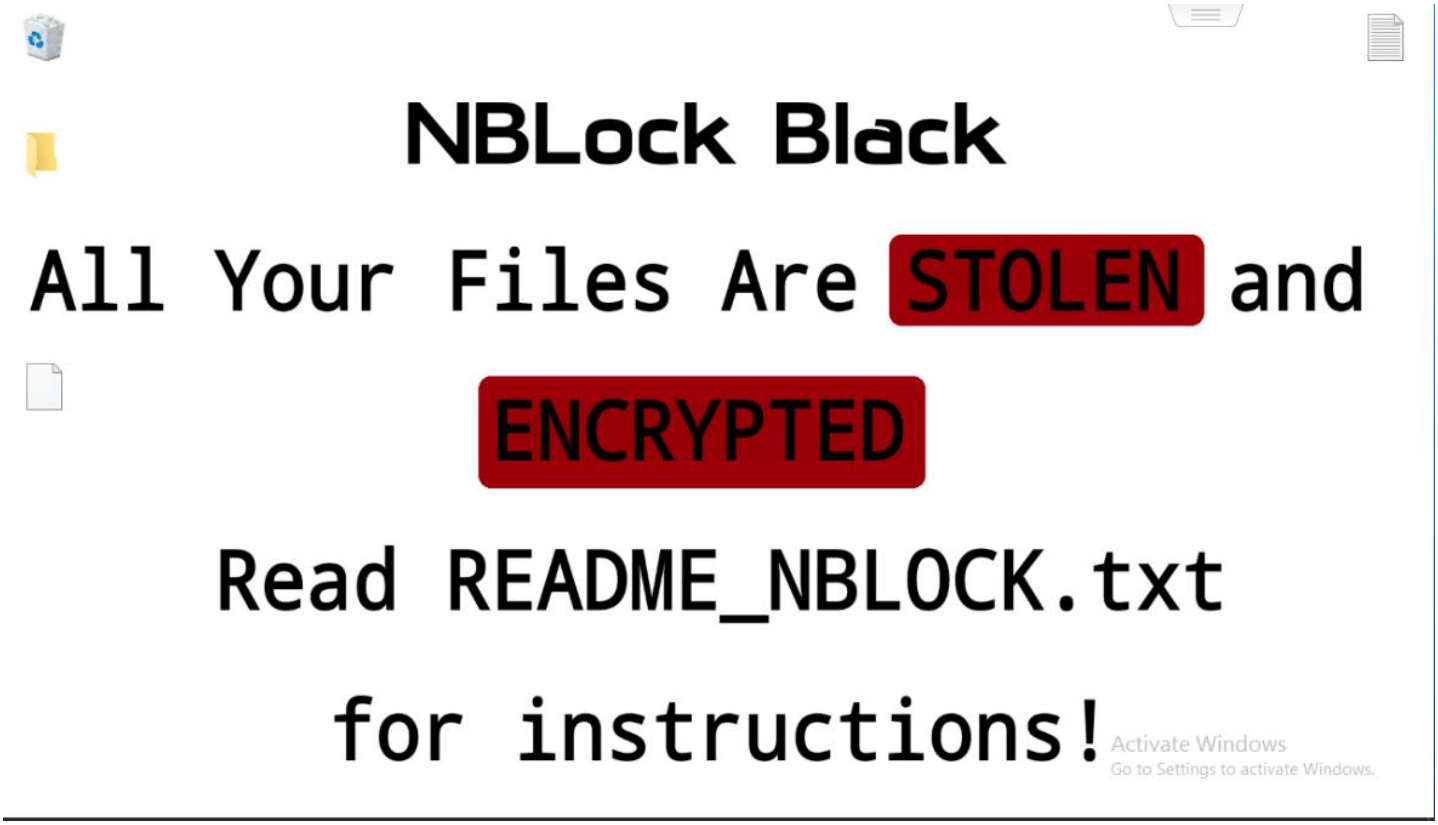


Image: Desktop wallpaper replaced with a full-screen notice claiming data theft and encryption.

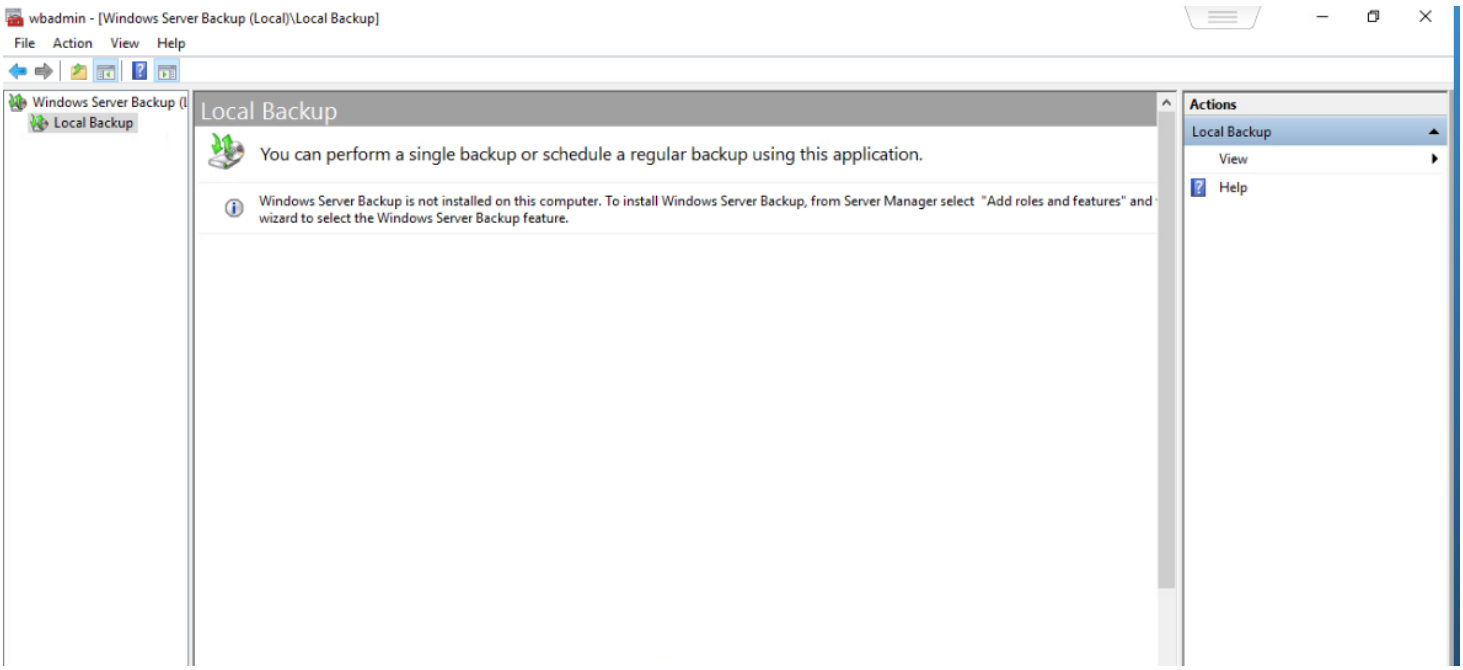
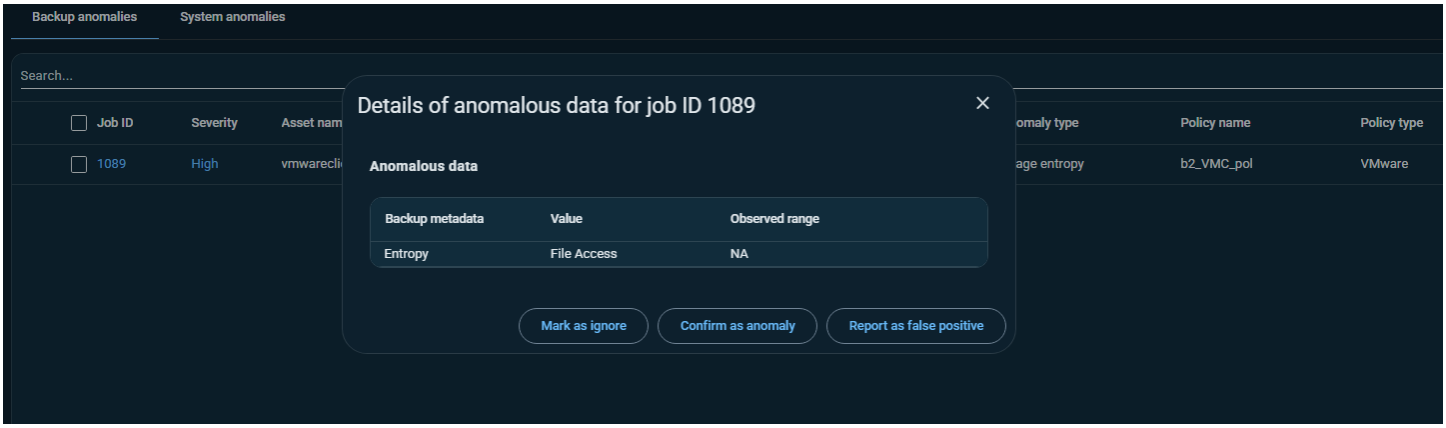


Image: Windows Server Backup reporting no local backup capability on the host after the attack.

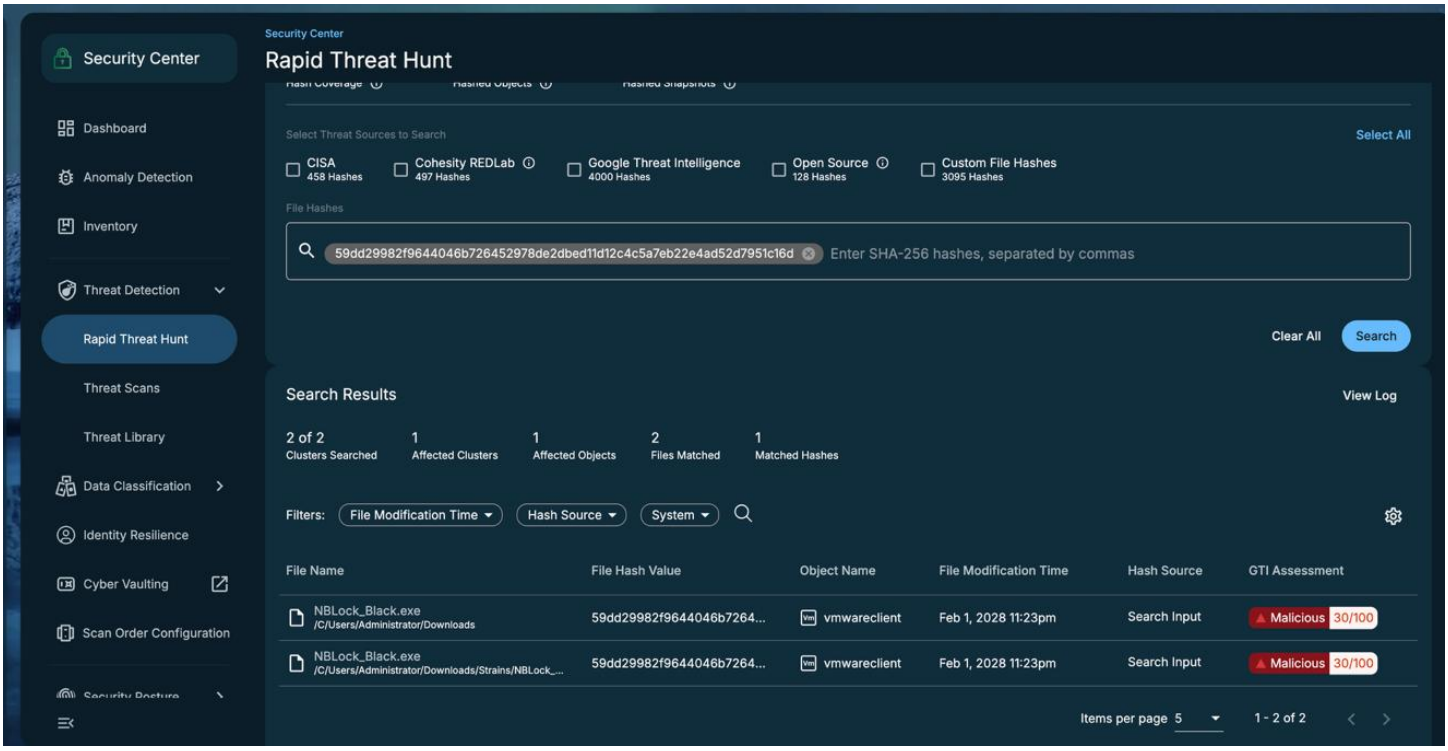
Protection & Detection Outcomes

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 NBLock Black 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.

Witch Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Data Encrypted for Impact	T1486	Impact
Inhibit System Recovery	T1490	Impact
Data Destruction	T1485	Impact
Impair Defenses	T1562	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Process Injection	T1055	Defense Evasion, Privilege Escalation
Hijack Execution Flow	T1574	Defense Evasion, Privilege Escalation, Persistence
Obfuscated Files or Information	T1027	Defense Evasion
Software Packing	T1027.002	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Windows Management Instrumentation	T1047	Execution
Command and Scripting Interpreter	T1059	Execution
Encrypted Channel	T1573	Command and Control
Application Layer Protocol	T1071	Command and Control
Process Discovery	T1057	Discovery
Software Discovery	T1518	Discovery
System Information Discovery	T1082	Discovery

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

Malware impact post execution

Witch is a 32-bit Windows .NET ransomware payload (approximately 145 KB) that pairs broad host reconnaissance with an unusually thorough recovery-sabotage routine. It performs anti-VM, anti-debugging and geofencing checks, then reconnoitres largely through native Windows utilities (WMI, cmdkey, netstat, tasklist, whoami, ipconfig) and enumerates AMSI providers as a likely precursor to EDR/AMSI bypass, clearing event logs throughout.

Encryption uses a hybrid AES/ChaCha20 scheme keyed to a victim identifier, appending a ".witch" extension; its "readme" ransom note demands payment in XMR or BTC and warns against tampering with files. Anti-recovery activity was the most aggressive observed this month: Witch deleted all volume shadow copies, disabled the Windows Recovery Environment, removed the Windows Server Backup catalog, disabled Windows Error Reporting, and rewrote boot configuration to suppress recovery alongside mass file deletion and staged exfiltration via external network callbacks.

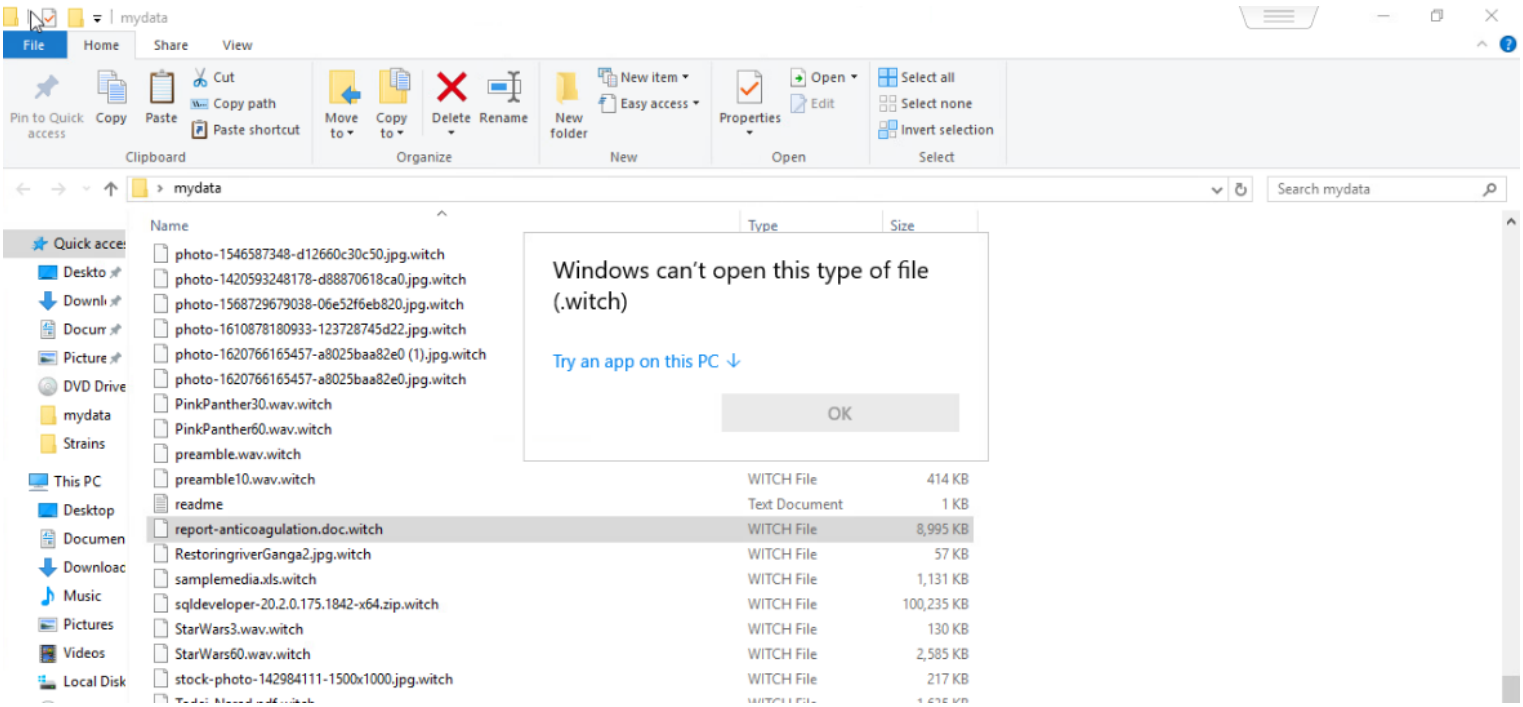


Image: Victim files following detonation, each appended with the ".witch" extension.

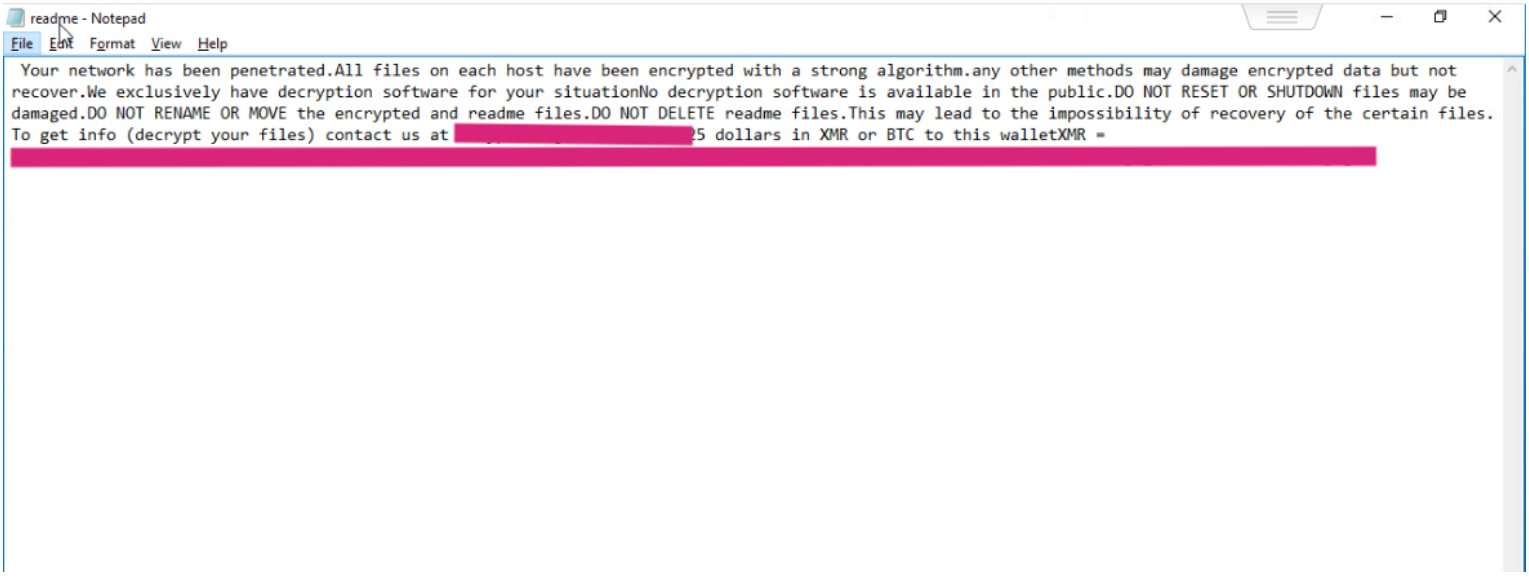


Image: The "readme" ransom note demanding payment in XMR or BTC and warning against renaming or deleting encrypted files.

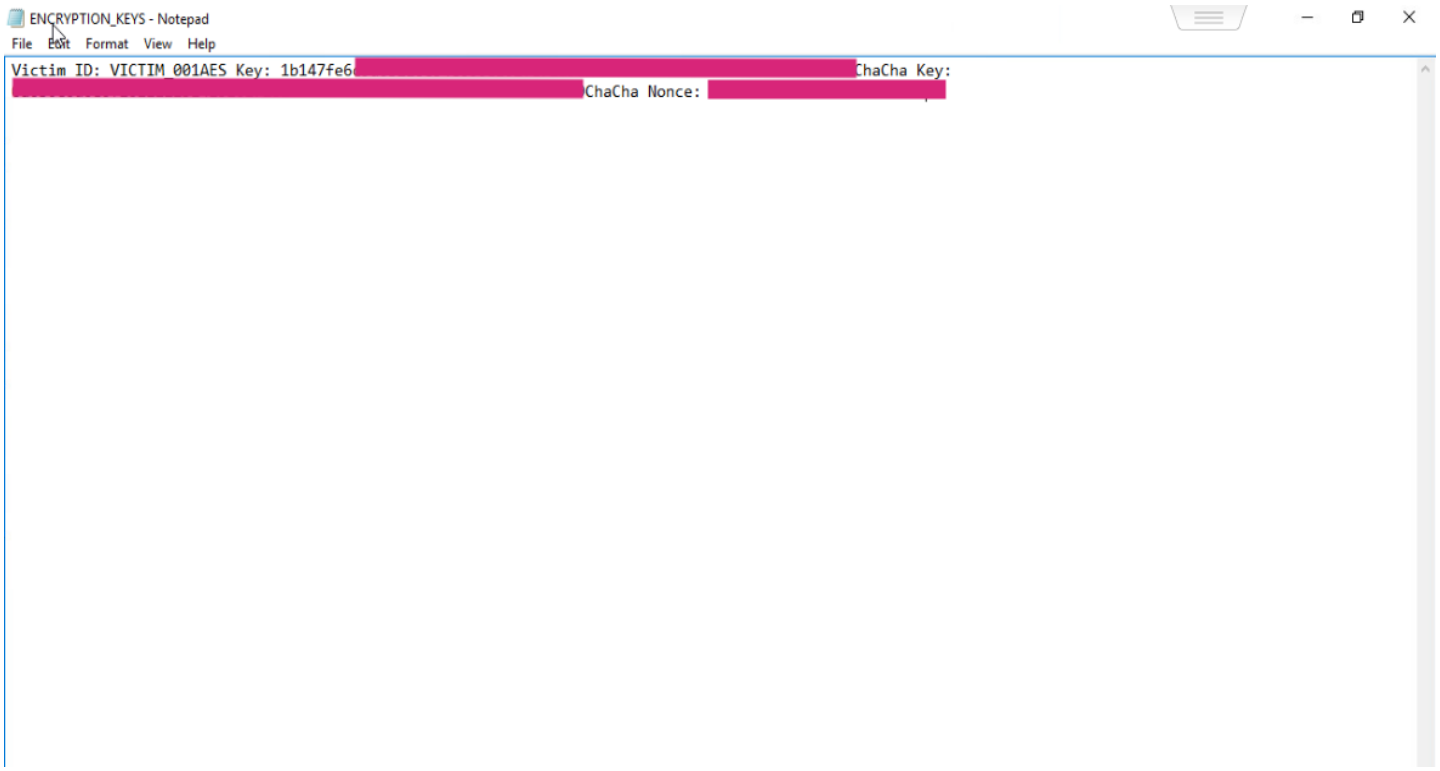


Image: The "ENCRYPTION_KEYS" artifact written during detonation, recording the victim ID alongside AES and ChaCha key material.

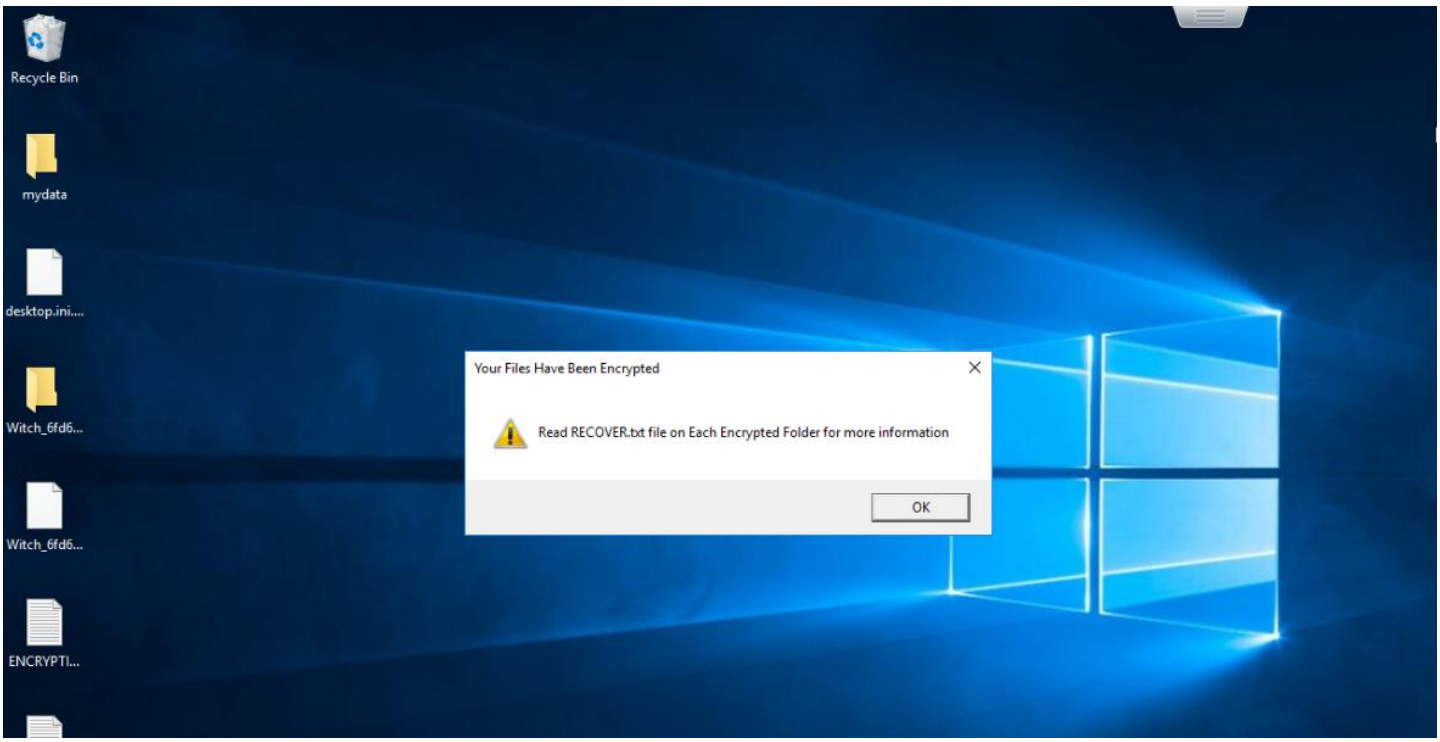
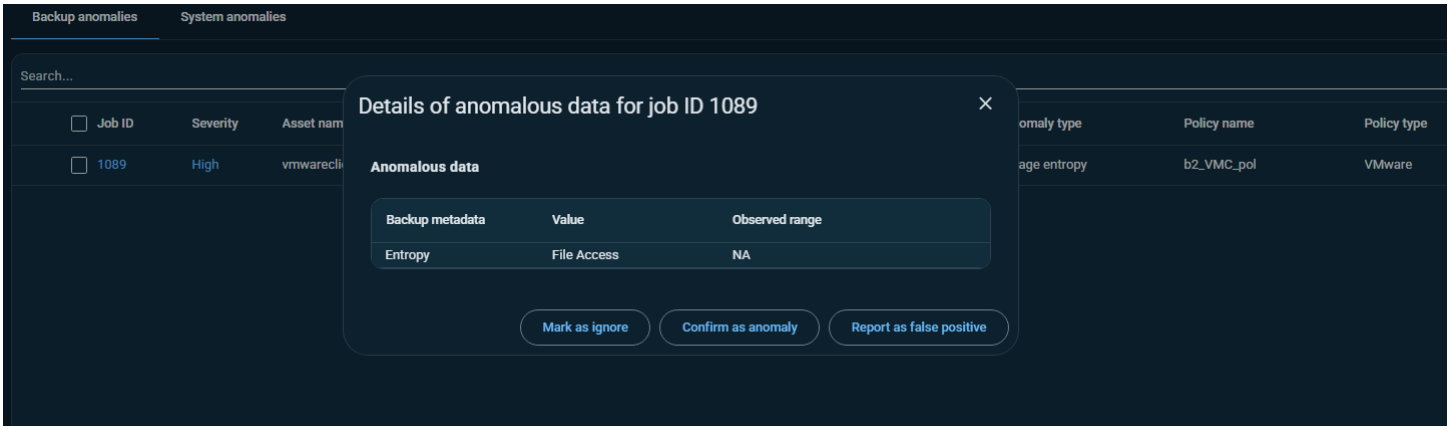


Image: On-screen notification presented to the victim after encryption completes, directing them to the dropped recovery instructions.

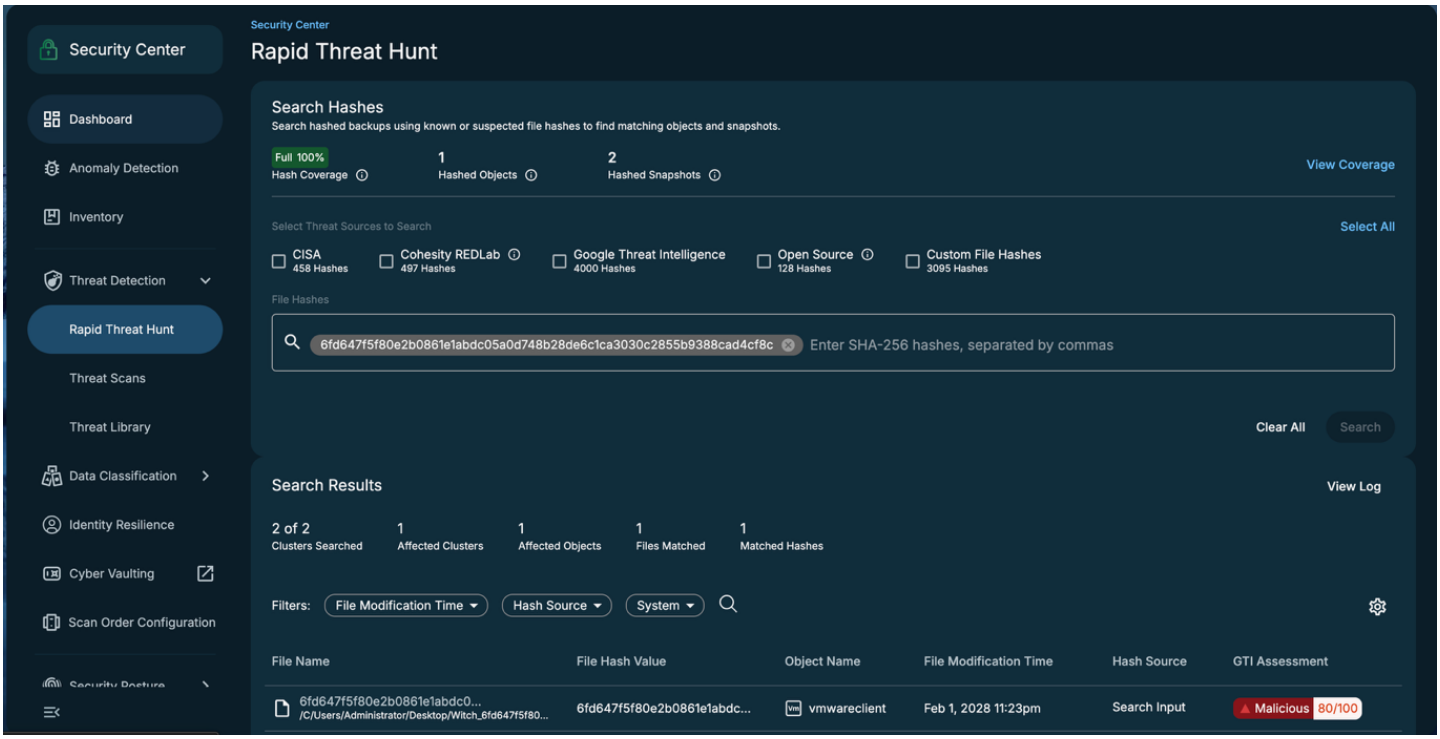
Protection & Detection Outcomes

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 Witch 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.

Gunra 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
Pre-OS Boot	T1542	Defense Evasion, Persistence
Rootkit	T1014	Defense Evasion
OS Credential Dumping	T1003	Credential Access
Credentials from Password Stores	T1555	Credential Access
Credentials from Web Browsers	T1555.003	Credential Access
Unsecured Credentials	T1552	Credential Access
Credentials In Files	T1552.001	Credential Access
Data from Local System	T1005	Collection
Abuse Elevation Control Mechanism	T1548	Defense Evasion, Privilege Escalation
Indicator Removal	T1070	Defense Evasion
Masquerading	T1036	Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Software Packing	T1027.002	Defense Evasion
Hidden Window	T1564.003	Defense Evasion
File and Directory Discovery	T1083	Discovery
System Information Discovery	T1082	Discovery

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

Malware impact post execution

Gunra is a 64-bit Windows PE ransomware payload (approximately 195 KB) associated with the ContiV2 code lineage. Before impact it checks for administrative/UAC elevation, profiles the host for geofencing, and enumerates processes, services and attached volumes from a hidden window.

Gunra is a double-extortion strain: it harvests browser credentials, password stores and file-based credentials, and enumerates user directories for staging, before encrypting over 1,300 files across the user profile, Public folder and attached volumes with a ".encrt" extension. Mass file deletion and overwriting also occurred. Its "R3ADM3.txt" ransom note is written into hundreds of directories, including the EFI system partition, and claims prior data exfiltration. Most significantly, the sample attempted to write directly to a physical drive, with pre-OS boot, bootkit and rootkit techniques attributed to the run targeting the boot chain itself and placing recovery beyond in-guest remediation.

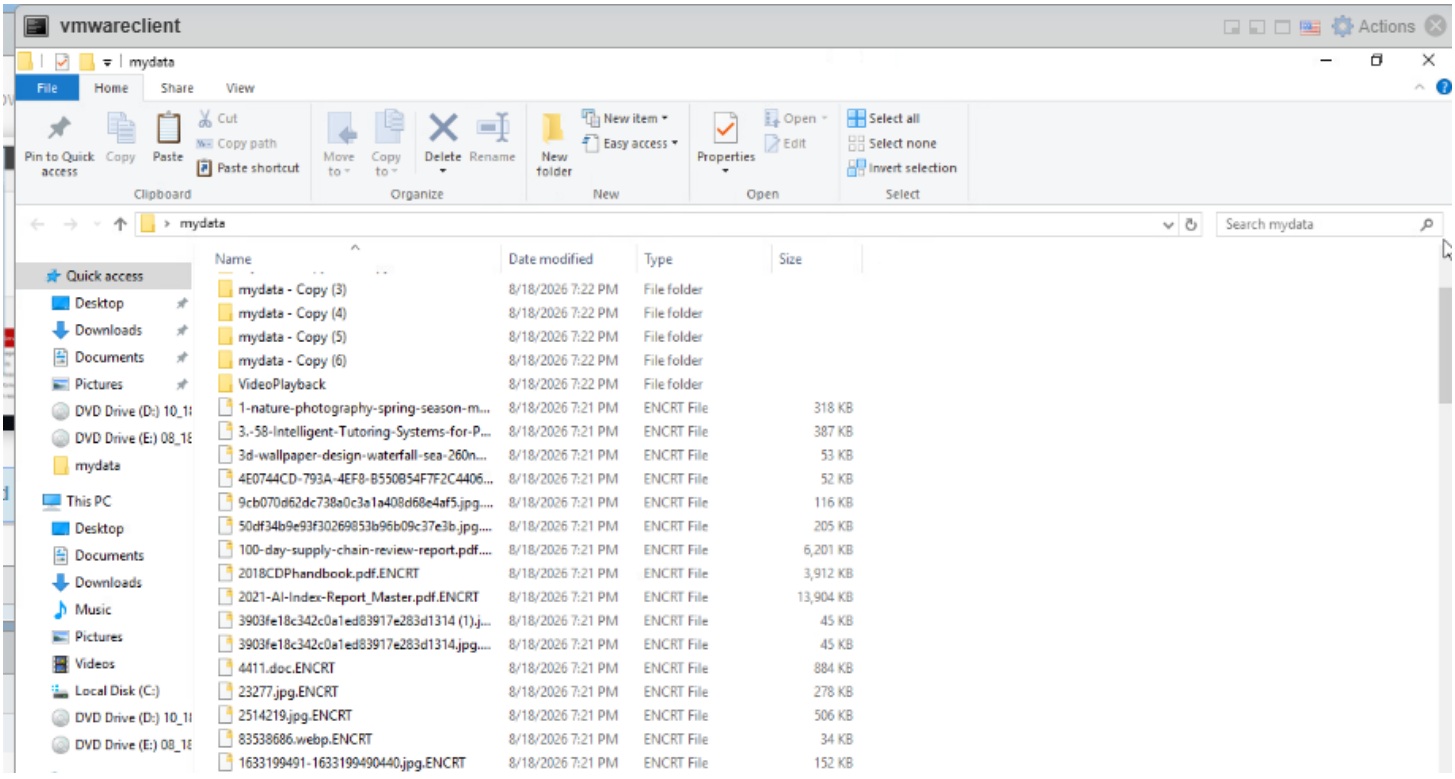


Image: Victim files following detonation, each appended with the ".encrt" extension.

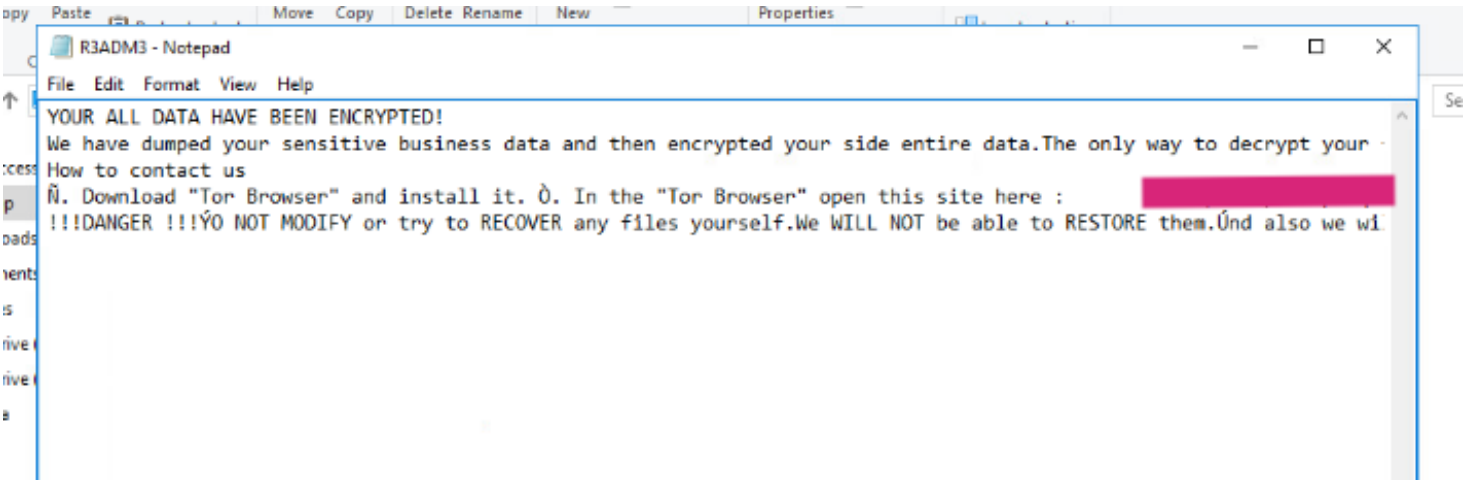
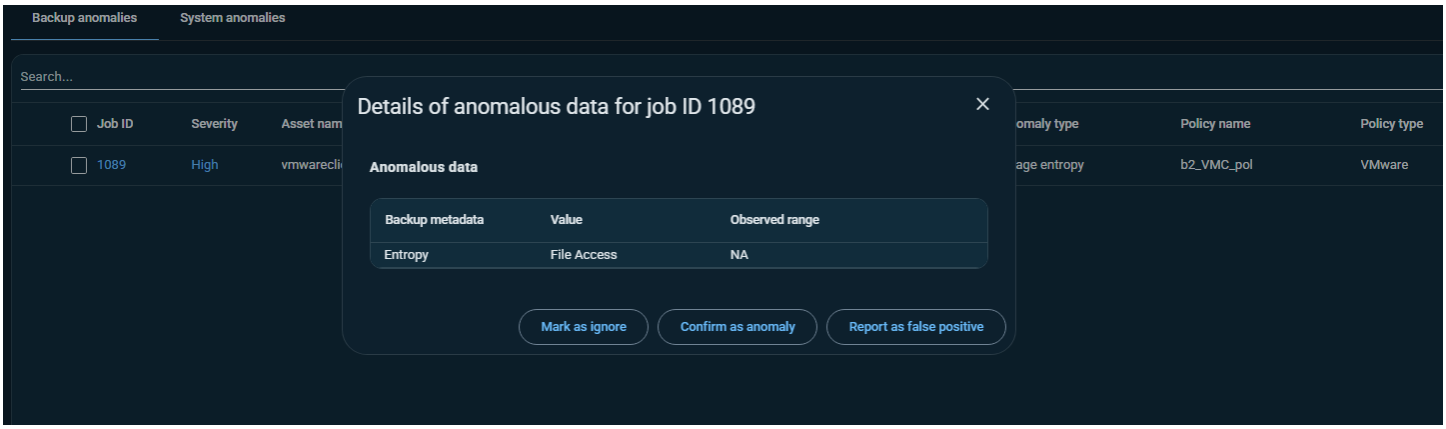


Image: The "R3ADM3.txt" ransom note claiming prior exfiltration of business data and directing the victim to a Tor hidden service.

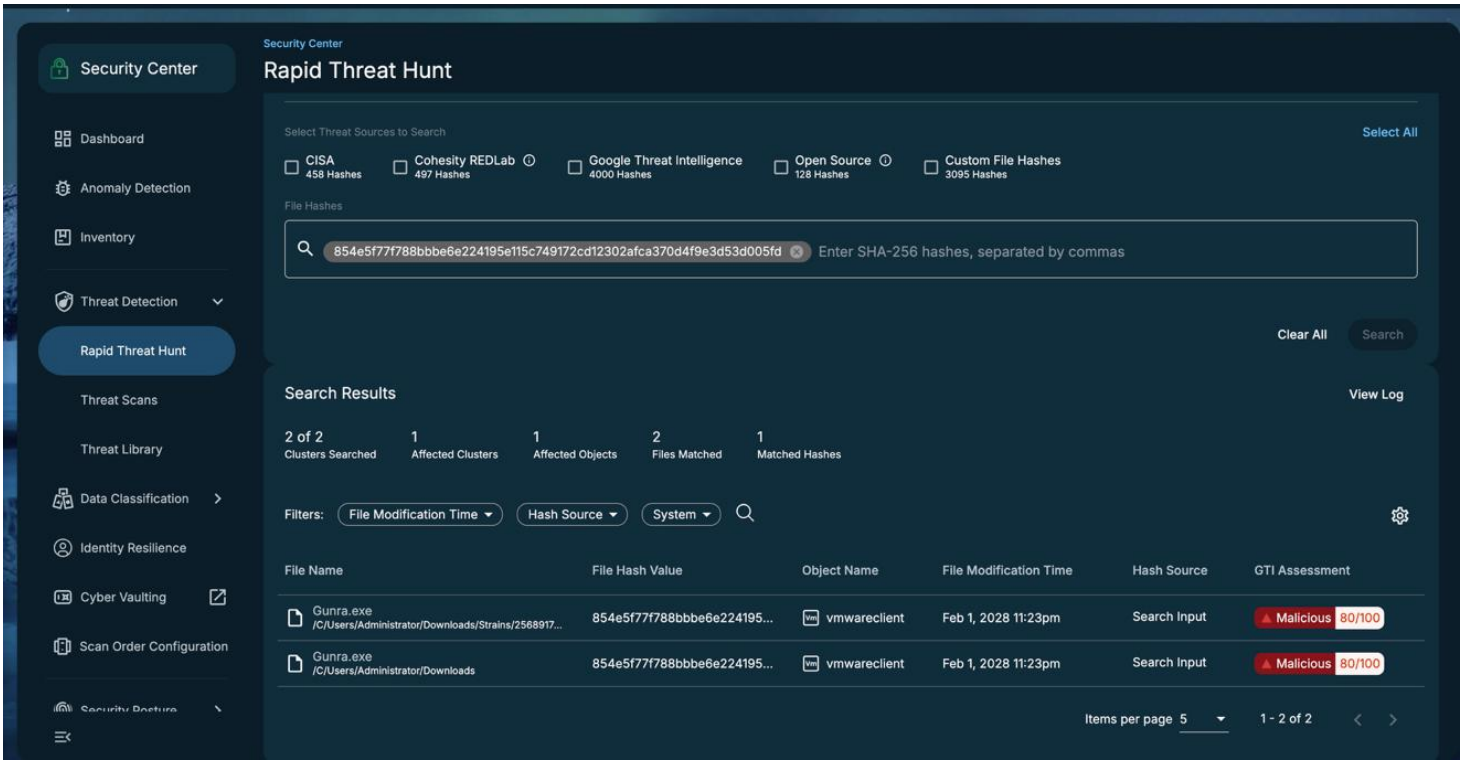
Protection & Detection Outcomes

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 Gunra 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 - LSD, NBLock Black, Witch and Gunra, 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