REDLab Product Security Newsletter

Cohesity REDLab is a dedicated team of security experts who perform in-depth research and rigorous malware testing inside a fully isolated environment. 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, and in turn, helps us build products that are more effective in data protection and security. The insights gained also provide valuable guidance to customer security and data protection teams.

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 effectiveness 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 testing against active, high-level cyber threats, not just theoretical threats or synthetic data.

- **Hardened Defense:** Testing in REDLab evaluates the security capabilities of DataProtect and NetBackup offer strong security capabilities. Positive results elevate the products beyond simple backup and recovery scenarios defence.

- **Forward-Looking:** REDLab continually broadens its testing scope in response to evolving threats. Further, REDLab uses the latest product innovations in advanced threat protection and threat hunting to benchmark performance against real-world 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: Absolute Domination Family: Absolute Domination Group	73e7290e2ff078283df8604817101904d1526895410314a505e2eeea43d215ce
Name: UNC Family: Dharma Ransomware Family	a2b997da39d37f8eb43947b4632cd2ae1886e434b8cc65ff8501d79080ab5f29
Name: End Family: MedusaLocker Ransomware Family	d387366313821a3e514d49dadd93b1fa4d6f3af6893ca19cb8c09e14dffcfe7e
Name: 0Apt_Locker Family: 0apt Locker Threat Group	844db4dfd04cd5fee440aba1323c46fea99a1cca9fdd6131099873414d70fc29

Absolute Domination Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Command and Scripting Interpreter	T1059	Execution
Shared Modules	T1129	Execution
Indirect Command Execution	T1202	Execution, Stealth
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Registry Run Keys / Startup Folder	T1547.001	Persistence, Privilege Escalation
Create or Modify System Process	T1543	Persistence, Privilege Escalation
Event Triggered Execution	T1546	Persistence, Privilege Escalation
Modify Registry	T1112	Persistence, Defense Evasion
Hijack Execution Flow	T1574	Privilege Escalation, Defense Evasion
Process Injection	T1055	Privilege Escalation, Defense Evasion
Impair Defenses	T1562	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Timestomp	T1070.006	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
System Owner/User Discovery	T1033	Discovery
System Information Discovery	T1082	Discovery
Application Layer Protocol	T1071	Command and Control
Service Stop	T1489	Impact
Inhibit System Recovery	T1490	Impact
Data Encrypted for Impact	T1486	Impact

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

Malware impact post execution

Absolute Domination surfaced in 2026 as a compact but aggressive ransomware strain built as a .NET Framework 4.7.2 (C#) PE32+ assembly rather than the Rust/native tooling seen in many modern families, signalling low-effort but effective "smash-and-grab" tradecraft. It recursively enumerates user directories and encrypts documents and media using AES (AesManaged) with PBKDF2-derived keys, appending a distinctive .dominated extension, and gates decryption behind a Windows Forms "locker" GUI password prompt while exfiltrating victim data via the Telegram Bot API. Before encrypting, it dismantles defenses disabling Windows Defender real-time, behavior and on-access monitoring, stopping AV services (WinDefend, wscsvc), and disabling Task Manager. It inhibits recovery through bcdedit commands and mass file overwrite/deletion and poisons the hosts file to null-route security and telemetry domains.

Image: Desktop Wallpaper updated post attack.

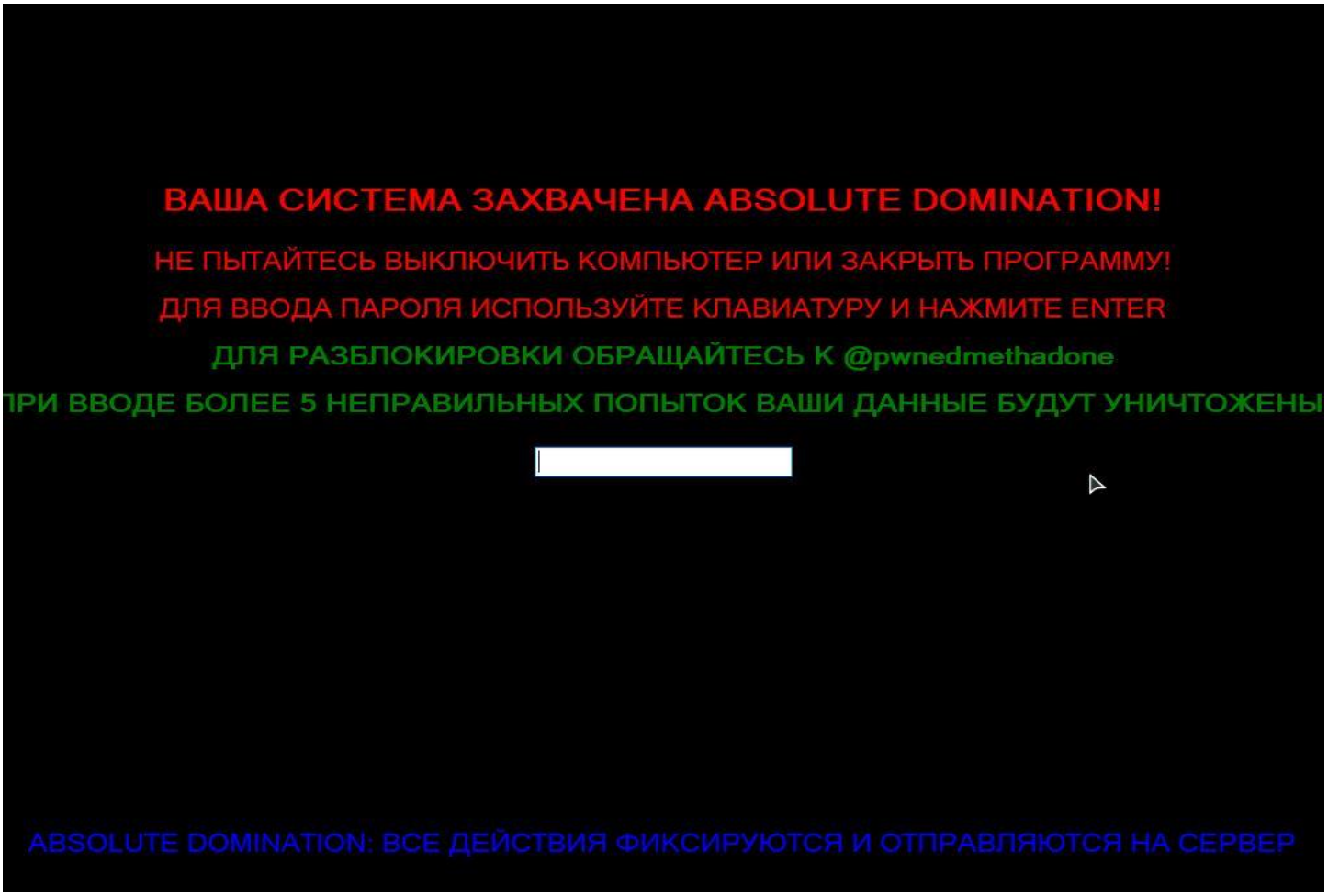
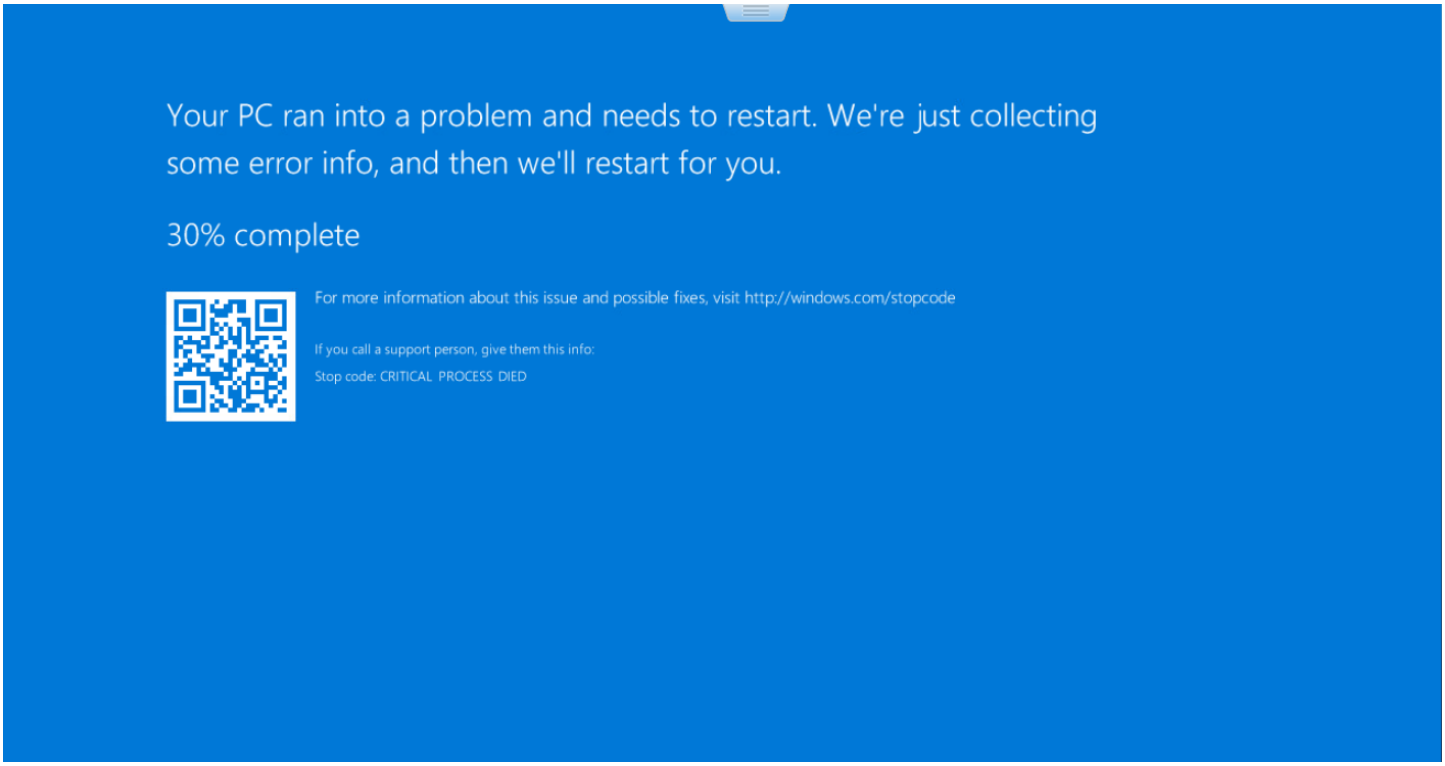
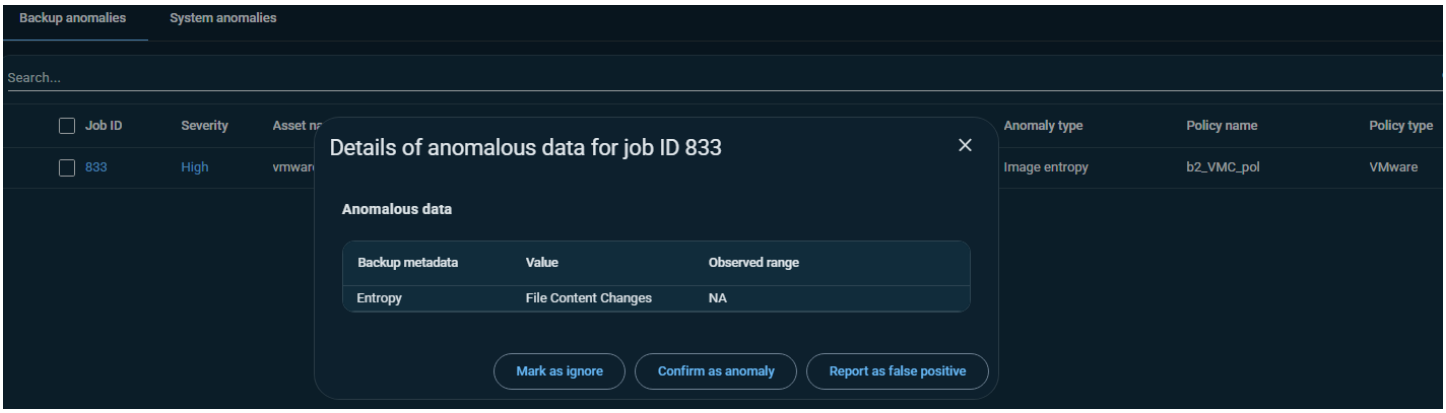


Image: VM crash (BSOD) with stop code CRITICAL_PROCESS_DIED, observed post attack.



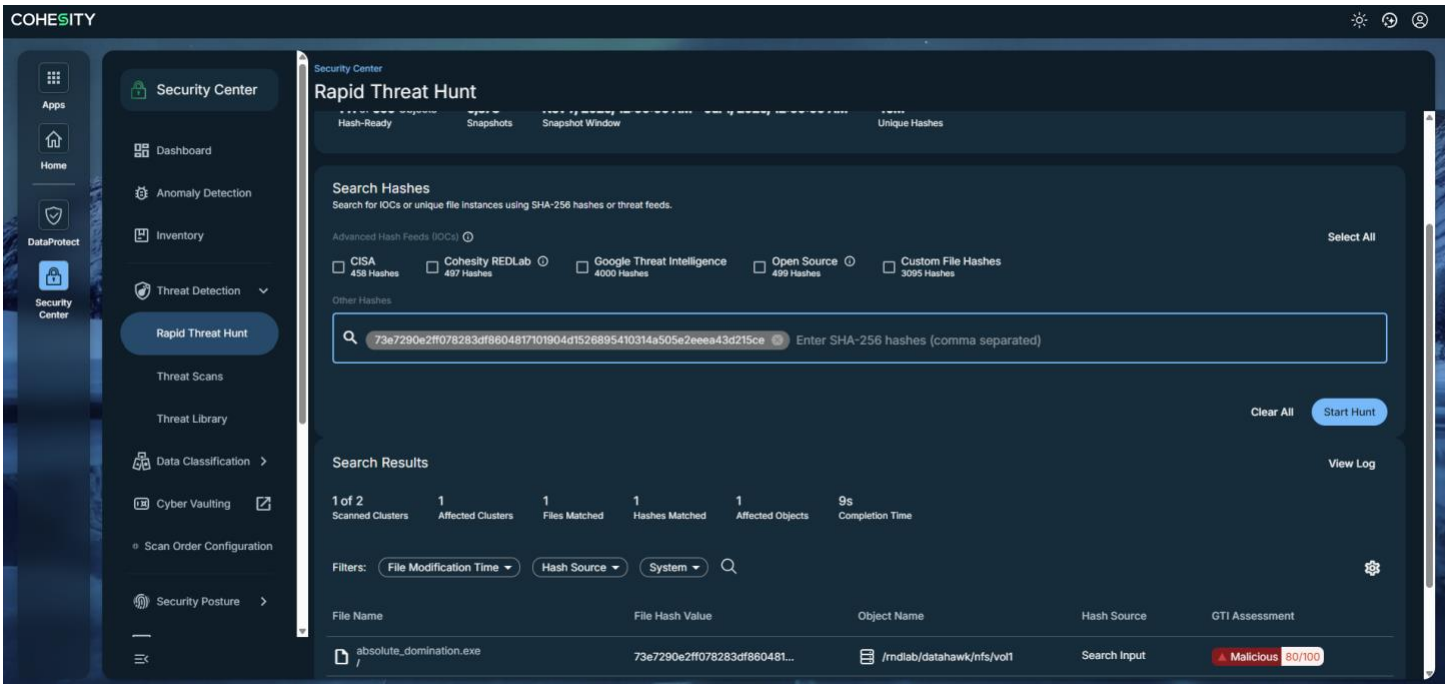
Outcomes

Both DataProtect and NetBackup completed successful VMware backup and recovery tasks 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 that its threat detection capabilities worked 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 Absolute Domination 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.

UNC Ransomware

Technique Name	MITRE ATT&CK ID	Tactic(s)
Shared Modules	T1129	Execution
Boot or Logon Autostart Execution	T1547	Persistence, Privilege Escalation
Modify Registry	T1112	Persistence, Defense Evasion
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
Indicator Removal	T1070	Defense Evasion
Indirect Command Execution	T1202	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Process Discovery	T1057	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
Data Staged	T1074	Collection
Application Layer Protocol	T1071	Command and Control
Data Destruction	T1485	Impact
Data Encrypted for Impact	T1486	Impact

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

Malware impact post execution

UNC ransomware is a recently observed ransomware variant belonging to the long-running Dharma (Crysis) ransomware family. After execution, it encrypts files on local systems and network-accessible shares, appending a distinctive ".UNC" extension together with a victim ID and attacker contact email (for example, ".id-XXXXXXXX.[cyberuncle@cyberfear.com].UNC"). It drops a ransom note and creates an "info.txt" file instructing victims to contact the operators via email for decryption. The malware employs classic double-extortion tactics, claiming that sensitive data has been stolen and threatening public disclosure if the ransom is not paid. Consistent with other Dharma variants, UNC disables or weakens system defenses, deletes Volume Shadow Copies to hinder recovery, and establishes persistence by copying itself into the %LOCALAPPDATA% directory and creating Windows Run registry entries. Its combination of file encryption, data-theft threats, recovery inhibition, and persistence mechanisms makes UNC a representative example of modern Dharma-based ransomware operations.

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

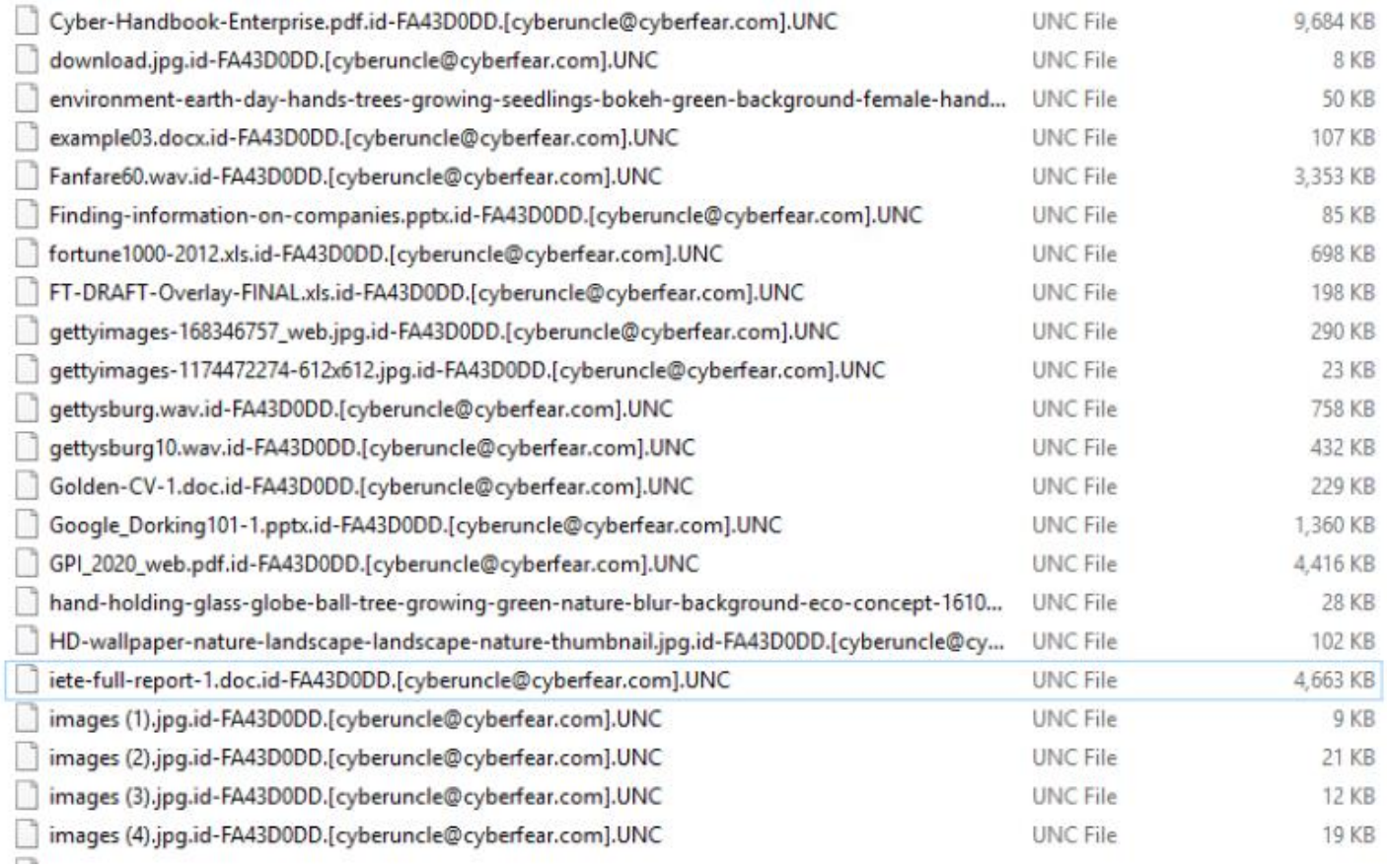
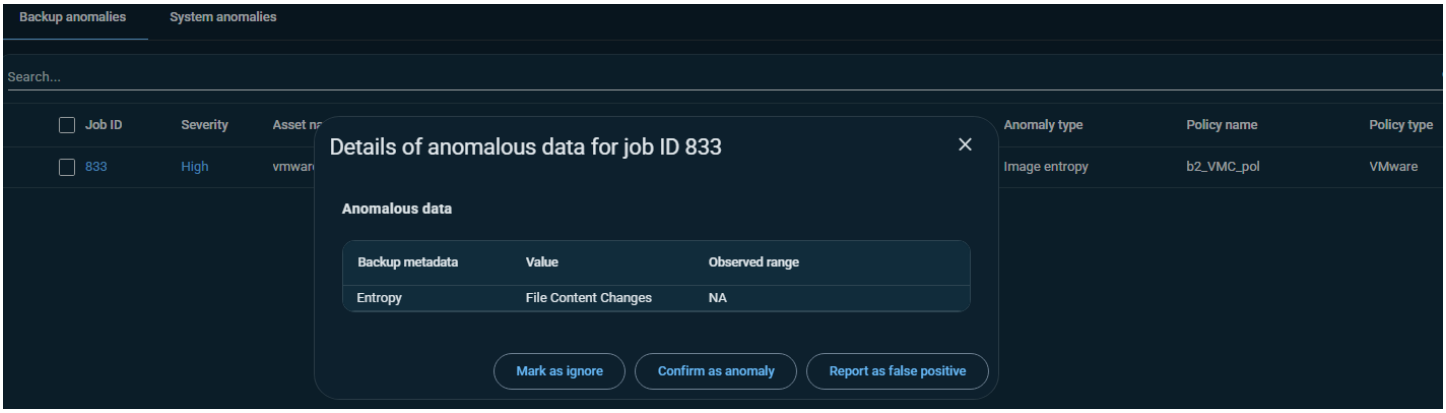


Image: UNC's ransom note (pop-up message)

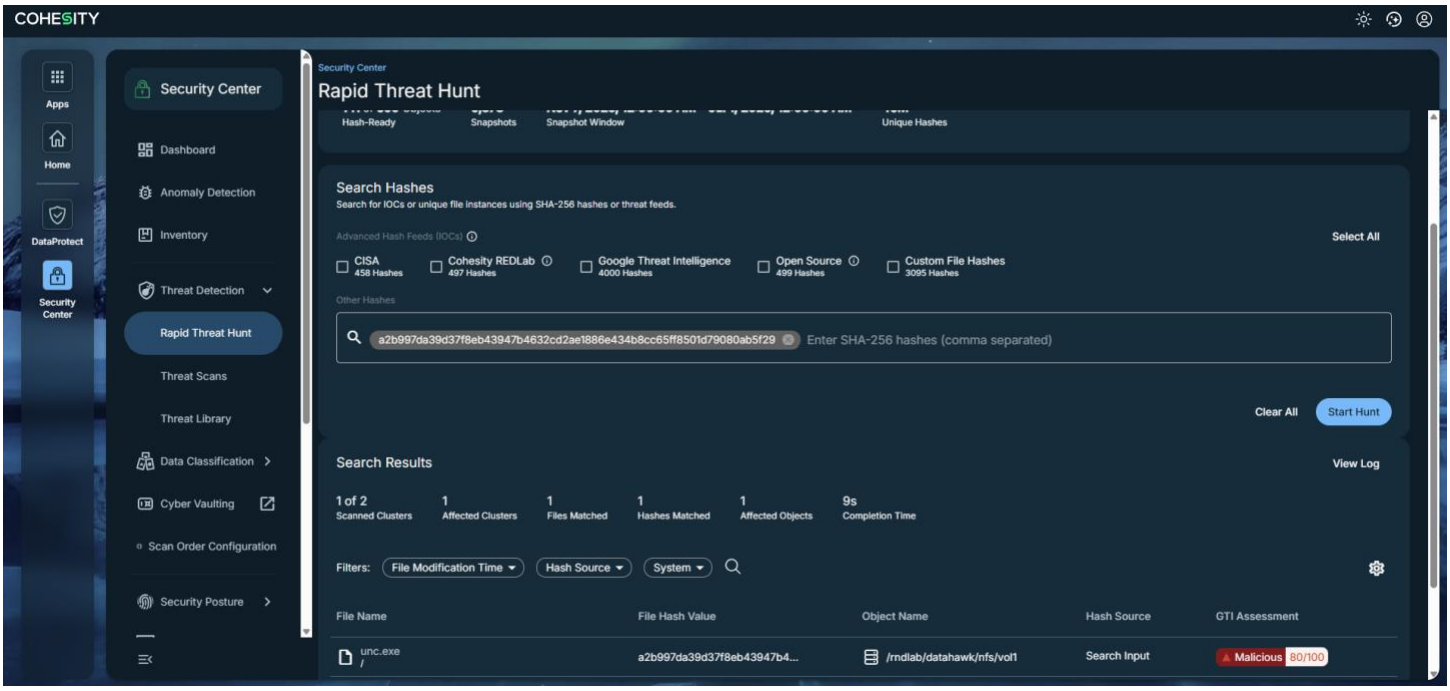
Outcomes

Both DataProtect and NetBackup completed successful VMware backup and recovery tasks following the attack. DataProtect VMware backup operations remained unaffected throughout. NetBackup's Image Entropy anomaly detection actively identified unusual deviations in VMware backup job attributes, demonstrating that its threat detection capabilities worked 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 UNC 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.

End 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
Deobfuscate/Decode Files or Information	T1140	Defense Evasion
Hide Artifacts	T1564	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
Virtualization/Sandbox Evasion	T1497	Defense Evasion, Discovery
Input Capture	T1056	Credential Access, Collection
Application Window Discovery	T1010	Discovery
Query Registry	T1012	Discovery
System Information Discovery	T1082	Discovery
File and Directory Discovery	T1083	Discovery
System Location Discovery	T1614	Discovery

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

Malware impact post execution

END is a native C/C++ 64-bit Windows ransomware behaving as a MedusaLocker-lineage variant that favours fast, high-coverage encryption over stealth. Post-execution it enumerates local, removable, and network volumes and encrypts files using a hybrid AES + RSA CryptoAPI scheme, using intermittent ("crypt-and-skip") encryption and a system-file skip-list to accelerate impact while keeping the host bootable. Every affected file is renamed with the .end11 extension, and a HOW_TO_RECOVER_DATA.html ransom note is dropped into every traversed directory with localised variants across dozens of language folders.

Image: Desktop wallpaper updated post attack, displaying attacker contact information.

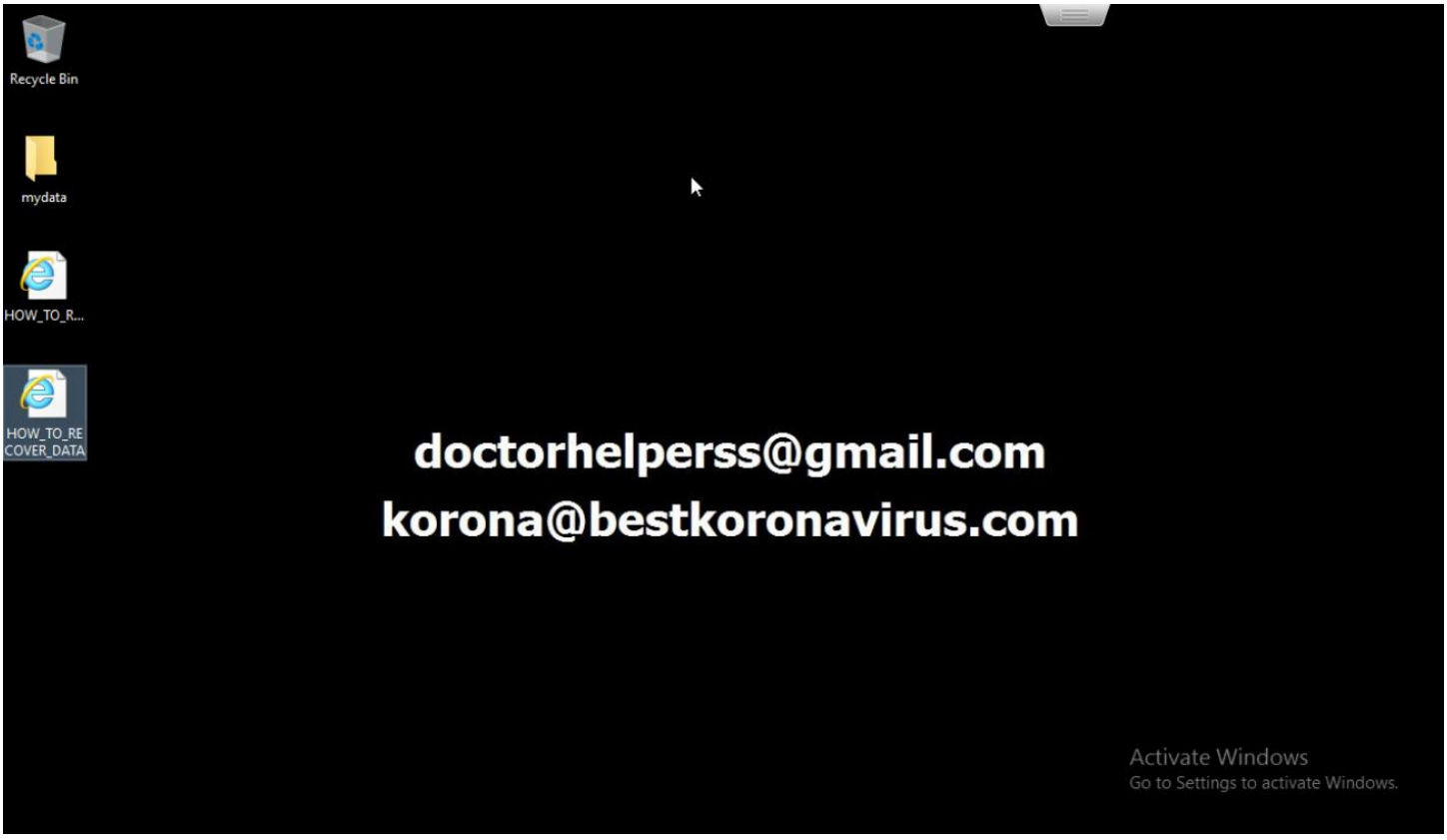
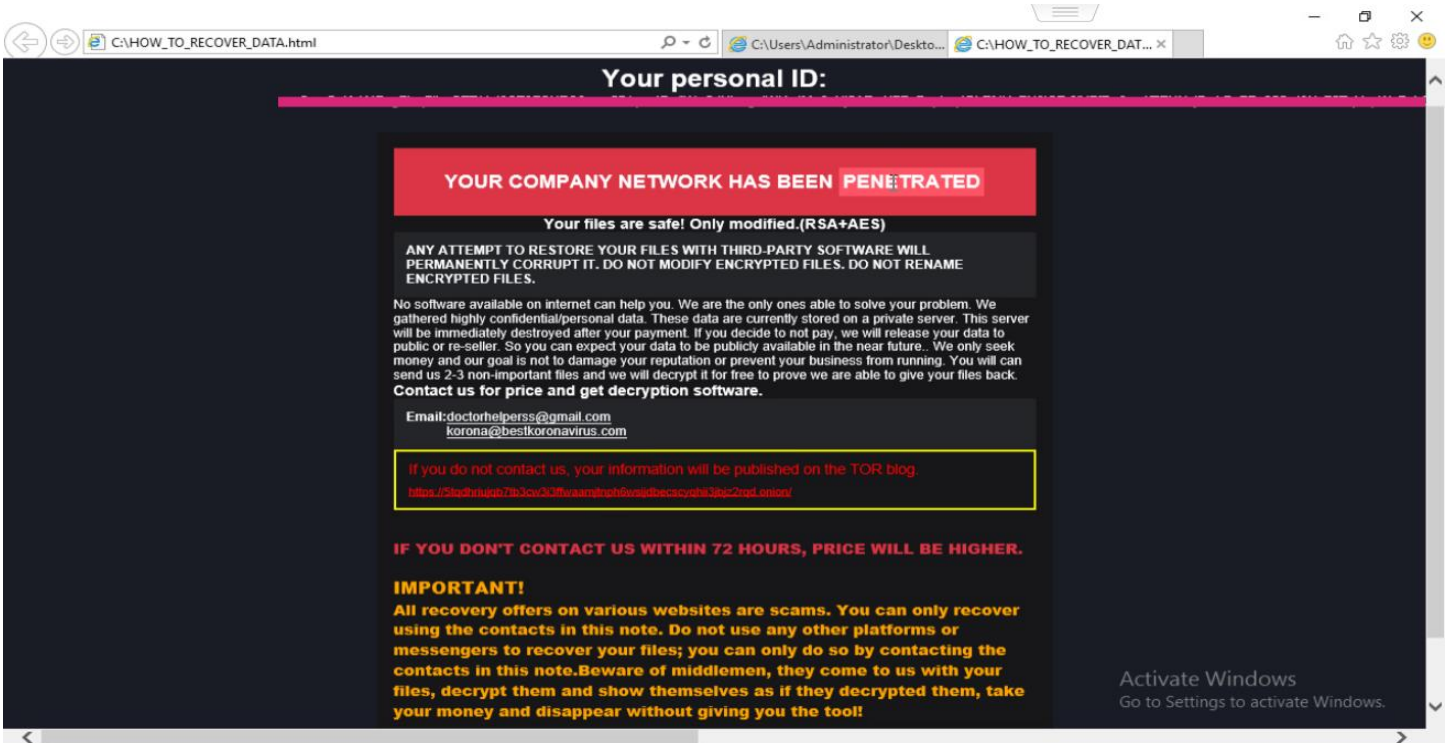
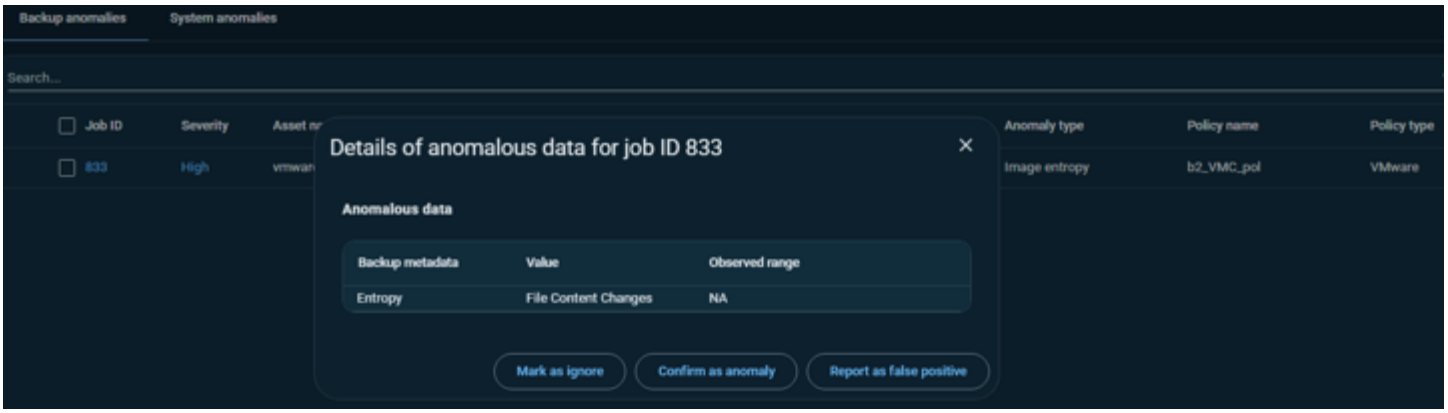


Image: Ransom Note named "HOW_TO_RECOVER_DATA.html" dropped along with recovery details.



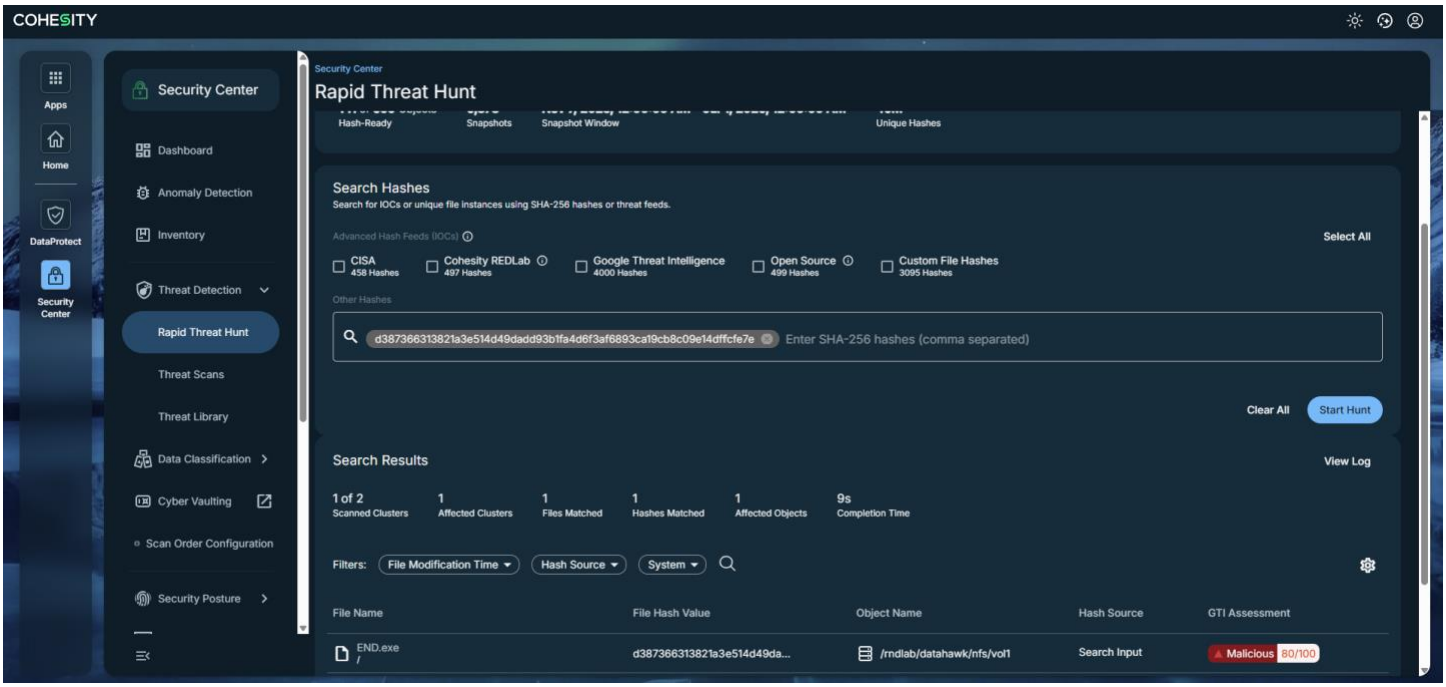
Outcomes

Both DataProtect and NetBackup completed successful VMware backup and recovery tasks 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 End 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.

0Apt_Locker Ransomware

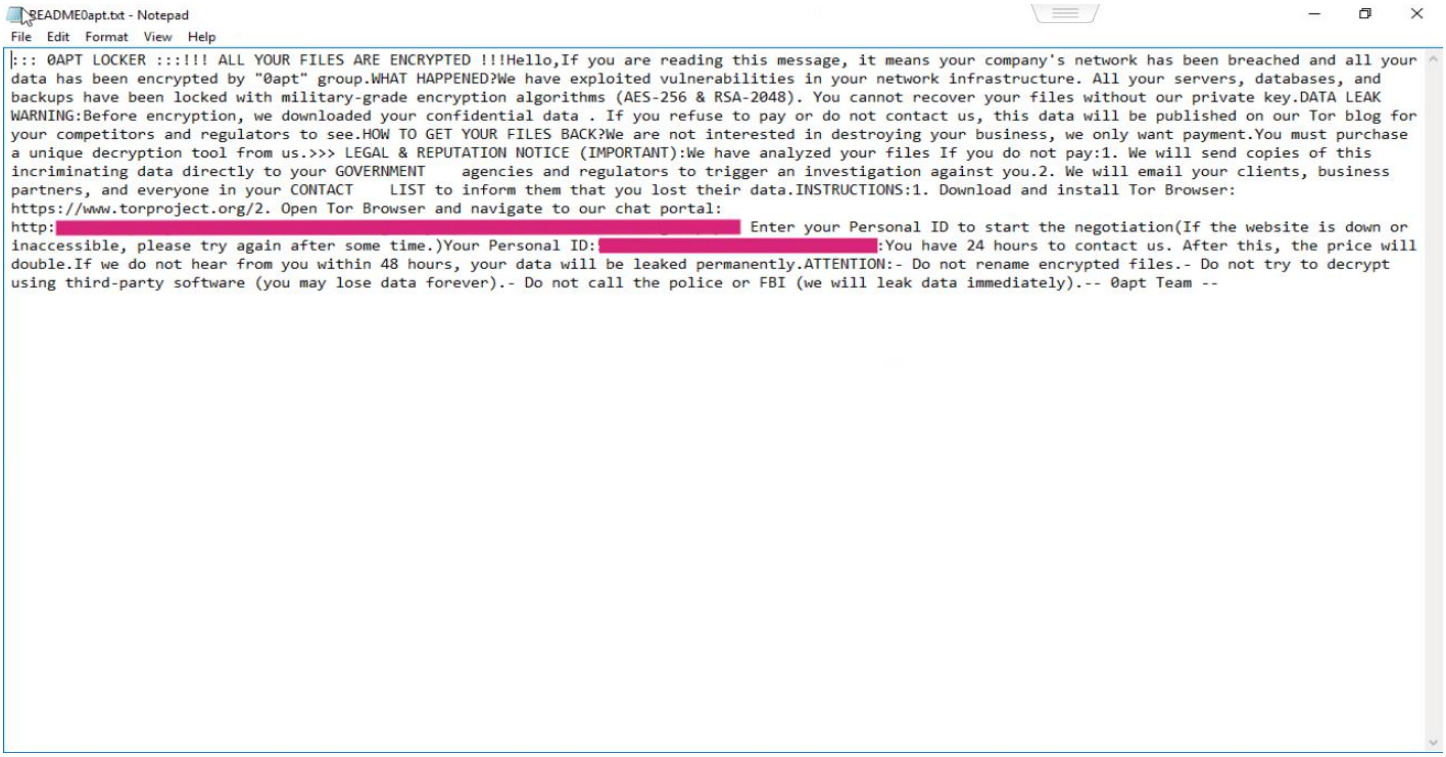
Technique Name	MITRE ATT&CK ID	Tactic(s)
Windows Management Instrumentation	T1047	Execution
Command and Scripting Interpreter	T1059	Execution
Native API	T1106	Execution
Shared Modules	T1129	Execution
Process Injection	T1055	Privilege Escalation, Defense Evasion
Abuse Elevation Control Mechanism	T1548	Privilege Escalation
Obfuscated Files or Information	T1027	Defense Evasion
Masquerading	T1036	Defense Evasion
File and Directory Permissions Modification	T1222	Defense Evasion
OS Credential Dumping	T1003	Credential Access
Unsecured Credentials	T1552	Credential Access
Query Registry	T1012	Discovery
System Network Configuration	T1016	Discovery
Process Discovery	T1057	Discovery

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

Malware impact post execution

0apt Locker is a Rust-built 64-bit Windows ransomware (~5.8 MB, with a leaked /home/kali/.cargo/ build path suggesting Linux-based development) that uses a robust hybrid encryption scheme. On execution it recursively walks the filesystem and encrypts files in parallel via a rayon thread pool for speed, applying AES (with AES-NI acceleration) to file contents and wrapping the keys with RSA-OAEP, making recovery infeasible without the attacker's private key. Encrypted files are renamed with the .0apt extension, and a ransom note named README0apt.txt is dropped across affected directories, directing victims to a Tor chat portal and applying double-extortion pressure by threatening to report them to agencies and regulators. It also overwrites the desktop wallpaper, enforces single-instance execution via a mutex, beacons over WinSock for command-and-control, and runs anti-VM, hardware-ID profiling, and anti-debug checks before detonation.

Image: Ransom Note named "README0apt.txt" dropped along with recovery details.

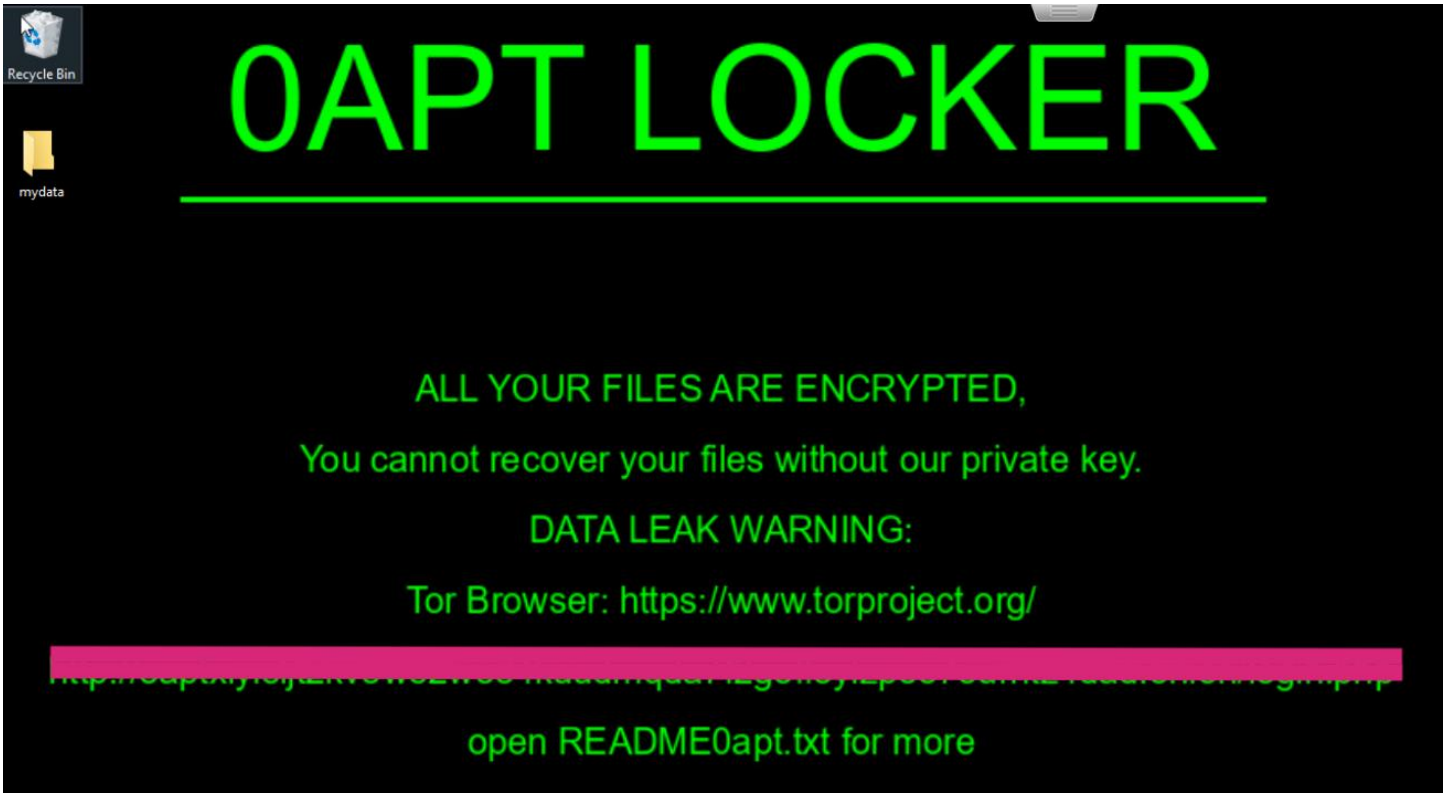

README0apt.txt - Notepad

File Edit Format View Help

::: 0APT LOCKER :::!!! ALL YOUR FILES ARE ENCRYPTED !!!Hello,If you are reading this message, it means your company's network has been breached and all your data has been encrypted by "0apt" group.WHAT HAPPENED?We have exploited vulnerabilities in your network infrastructure. All your servers, databases, and backups have been locked with military-grade encryption algorithms (AES-256 & RSA-2048). You cannot recover your files without our private key.DATA LEAK WARNING:Before encryption, we downloaded your confidential data . If you refuse to pay or do not contact us, this data will be published on our Tor blog for your competitors and regulators to see.HOW TO GET YOUR FILES BACK?We are not interested in destroying your business, we only want payment.You must purchase a unique decryption tool from us.>>> LEGAL & REPUTATION NOTICE (IMPORTANT):We have analyzed your files If you do not pay:1. We will send copies of this incriminating data directly to your GOVERNMENT agencies and regulators to trigger an investigation against you.2. We will email your clients, business partners, and everyone in your CONTACT LIST to inform them that you lost their data.INSTRUCTIONS:1. Download and install Tor Browser: https://www.torproject.org/2. Open Tor Browser and navigate to our chat portal:

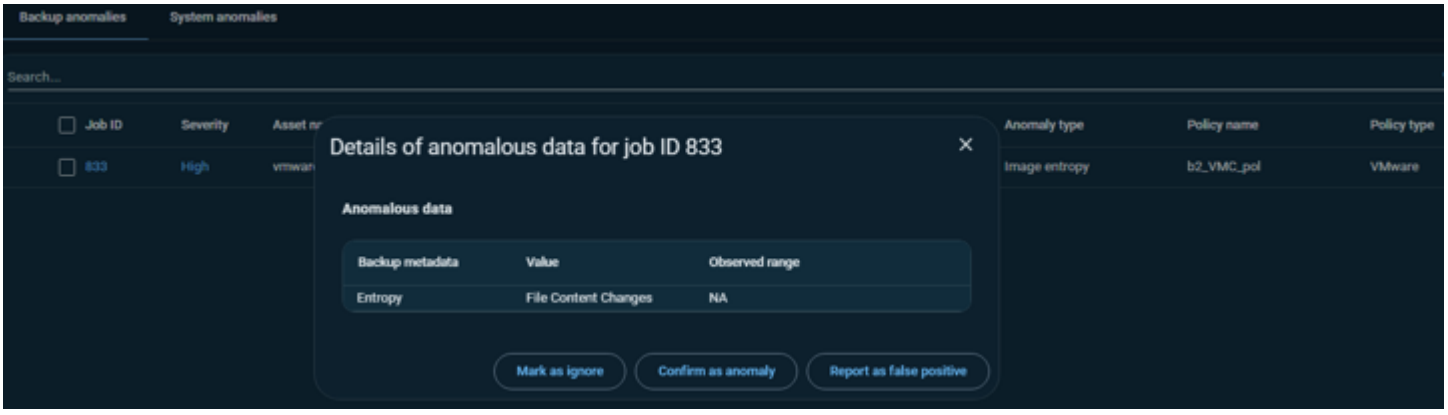
http:[redacted] Enter your Personal ID to start the negotiation(If the website is down or inaccessible, please try again after some time.)Your Personal ID:[redacted]:You have 24 hours to contact us. After this, the price will double.If we do not hear from you within 48 hours, your data will be leaked permanently.ATTENTION:- Do not rename encrypted files.- Do not try to decrypt using third-party software (you may lose data forever).- Do not call the police or FBI (we will leak data immediately).-- 0apt Team --

Image: Desktop wallpaper updated post attack, displaying "0APT LOCKER" branding.



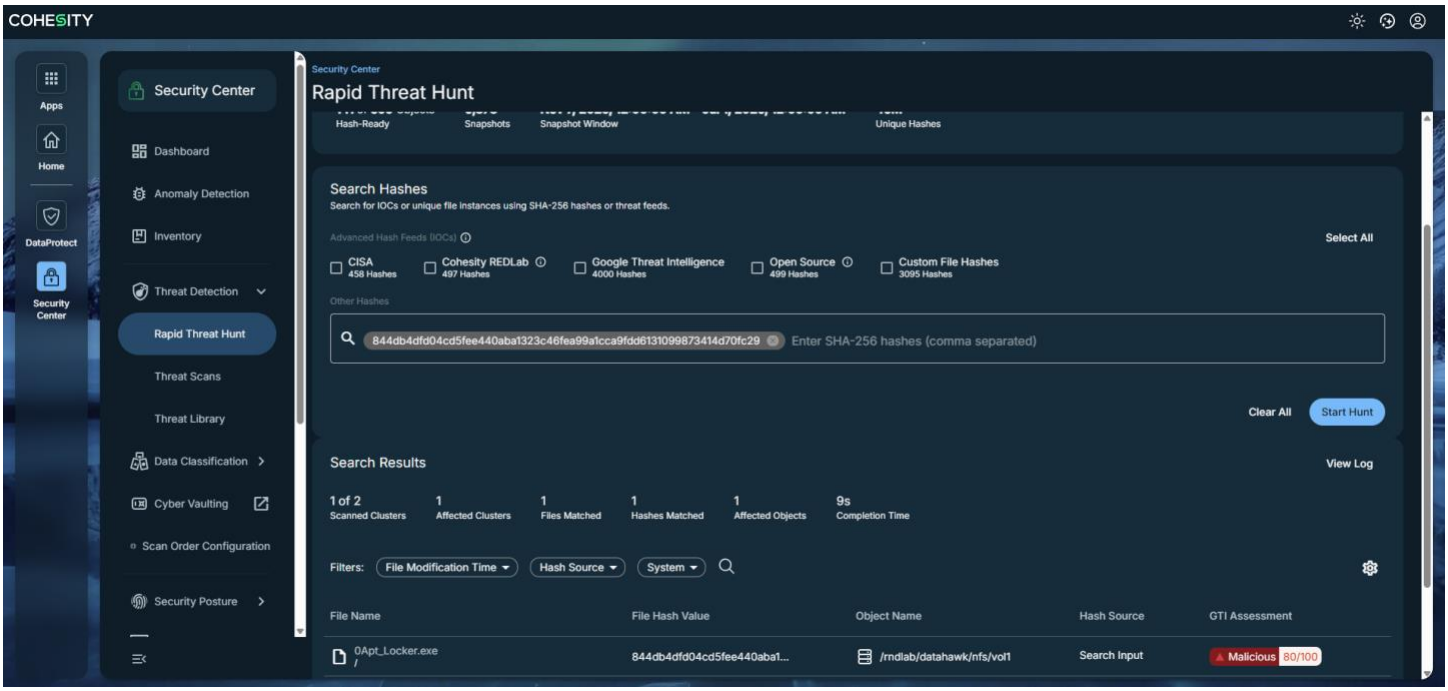
Outcomes

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 0Apt_Locker 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 completed VMware backup and recovery job successfully across all four ransomware strains tested - Absolute Domination, UNC, End and 0Apt_Locker, demonstrating the reliability 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 that its active threat detection capabilities work 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