Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

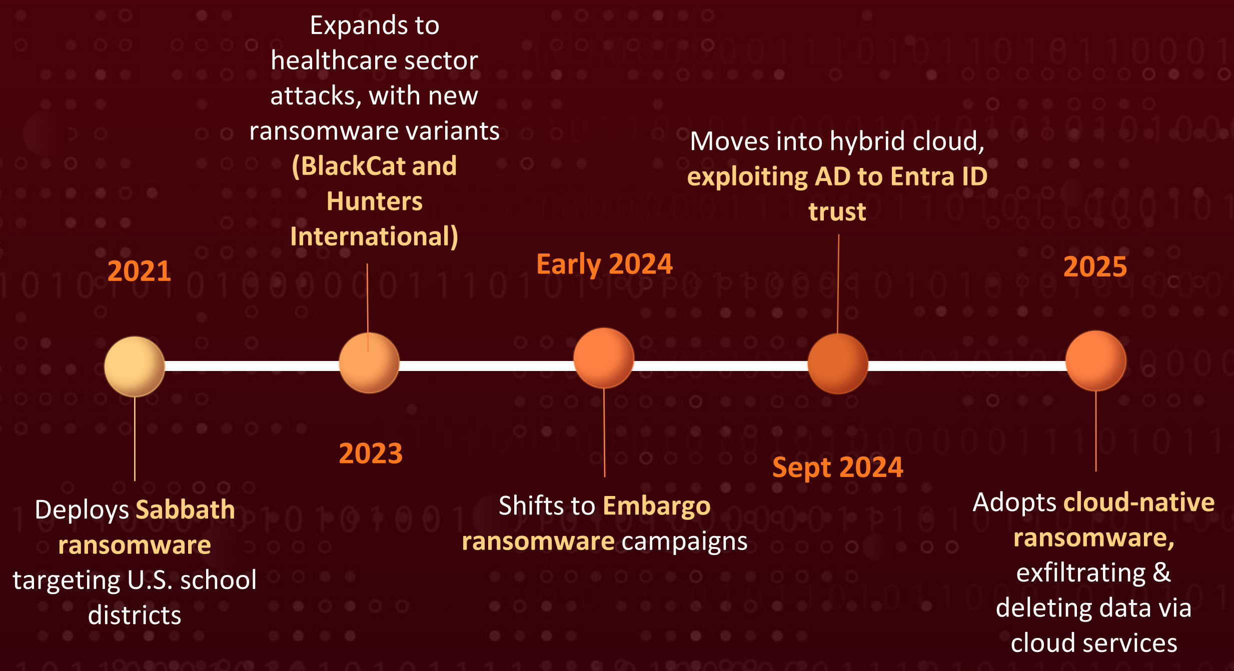
Storm-0501's Shift to Cloud-Native Ransomware

Date of Publication	Admiralty Code	TA Number
August 29, 2025	A1	TA2025264

Summary

First Seen: 2021
Targeted Countries: Worldwide
Targeted Platforms: Windows
Threat Actor: Storm-0501
Targeted Industries: Critical infrastructure, Government, Law enforcement, Energy, Aerospace, Defense, Healthcare, and Financial services, Agriculture, Media, and Consumer goods
Attack: Storm-0501, active since 2021, has shifted from traditional ransomware to cloud-based attacks, exploiting identity misconfigurations and fragmented security in hybrid environments. In a recent campaign, the group abused gaps in cloud identity and security tool deployment to escalate privileges and execute ransomware directly in the cloud. Instead of relying on endpoint malware, they exfiltrated data, deleted backups, and enforced ransom demands through cloud-native operations. Organizations are advised to strengthen identity security, unify security controls, and close visibility gaps to counter this evolving threat.

Threat Actor's Timeline



2021

Deploys **Sabbath ransomware** targeting U.S. school districts

2023

Expands to healthcare sector attacks, with new ransomware variants **(BlackCat and Hunters International)**

Early 2024

Shifts to **Embargo ransomware** campaigns

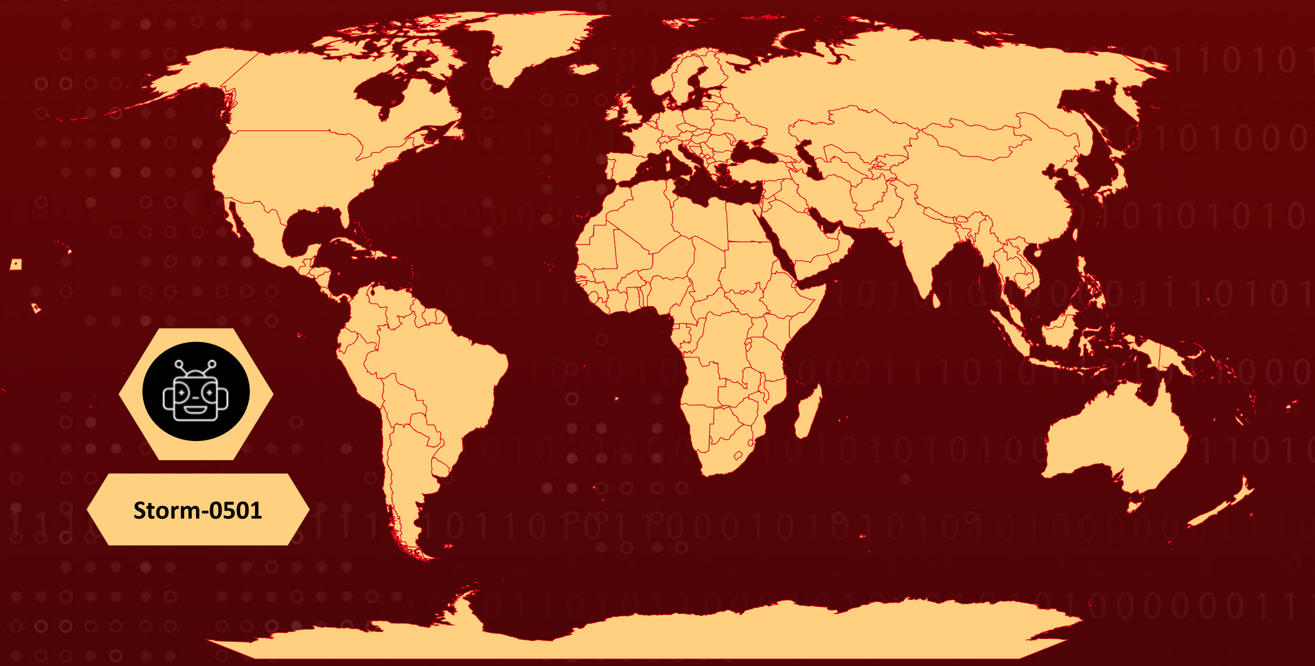
Sept 2024

Moves into hybrid cloud, **exploiting AD to Entra ID trust**

2025

Adopts **cloud-native ransomware,** exfiltrating & deleting data via cloud services

Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

Storm-0501 is a financially motivated threat actor that has evolved from traditional endpoint-based ransomware to sophisticated cloud-native campaigns, actively targeting organizations with hybrid environments. Instead of relying on malware to encrypt files on-premises, they exploit cloud capabilities to exfiltrate and destroy large volumes of data, bypassing conventional security controls and making remediation far more difficult. Storm-0501 targets globally, but most targeted countries include the United States, the United Kingdom, Germany, Australia, Kenya, Bangladesh, and Peru.

#2

Their attacks often begin with the compromise of an on-premises Active Directory domain through privilege escalation and credential theft. After achieving domain administrator access, Storm-0501 pivots to the cloud by abusing Entra Connect Sync accounts, enumerating cloud users and resources, and hijacking privileged identities. By resetting passwords and registering new MFA methods, they secure persistence and expand control.

#3

With global administrator privileges, Storm-0501 escalates their reach across Azure subscriptions, exposing storage accounts, stealing access keys, and deleting or exfiltrating backups. They attempt to bypass safeguards like resource locks or immutability, and in some cases even leverage Azure Key Vaults to encrypt cloud data and block recovery.

#4

The final phase is extortion: after crippling the victim's cloud environment, Storm-0501 uses compromised collaboration tools, such as Microsoft Teams accounts, to deliver ransom demands. This cloud-centric methodology underscores the need for organizations to enforce strong identity protections, unify monitoring across tenants, and mandate multi-factor authentication for all privileged accounts.

Recommendations

On-Premises Protection: Enable tamper protection and run endpoint detection and response (EDR) in block and automated remediation modes to prevent lateral movement and malware persistence. Keep software patched, especially enterprise tools like Zoho ManageEngine. Monitor privileged accounts and block abuse of admin tools.

Cloud Identity Security: Enforce multifactor authentication (MFA) with phishing-resistant methods on all accounts, especially privileged users. Apply Conditional Access policies to limit access from untrusted IPs and devices. Restrict and audit Directory Synchronization Account permissions and enforce least privilege on all cloud identities.

Cloud Resource Safeguards: Use Microsoft Defender for Cloud to monitor Azure resources and enable resource locks and immutable storage policies to prevent unauthorized or accidental deletions. Enable backup solutions and private endpoints to secure storage accounts. Protect Azure Key Vaults with purge protection and logging.

General Hygiene and Monitoring: Use security exposure management to identify critical assets and assess attack paths. Continuously monitor authentication and cloud activity for anomalies and signs of compromise. Train users to recognize phishing, and maintain strong password policies and backup procedures to enable quick recovery from attacks.

Potential MITRE ATT&CK TTPs

TA0040 Impact	TA0001 Initial Access	TA0002 Execution	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0010 Exfiltration	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection
T1567.002 Exfiltration to Cloud Storage	T1530 Data from Cloud Storage	T1486 Data Encrypted for Impact	T1485 Data Destruction
T1484 Domain Policy Modification	T1134 Access Token Manipulation	T1562.001 Disable or Modify Tools	T1562 Impair Defenses
T1484.002 Domain Trust Modification	T1134.002 Create Process with Token	T1003.006 DCSync	T1482 Domain Trust Discovery
T1059 Command and Scripting Interpreter	T1133 External Remote Services	T1078 Valid Accounts	T1078.004 Cloud Accounts
T1059.009 Cloud API	T1098.003 Additional Cloud Roles	T1098 Account Manipulation	T1003 OS Credential Dumping
T1586 Compromise Accounts	T1586.003 Cloud Accounts	T1136.001 Local Account	T1059.001 PowerShell

T1136 Create Account	T1087 Account Discovery	T1087.002 Domain Account	T1021 Remote Services
T1567 Exfiltration Over Web Service	T1053.005 Scheduled Task	T1053 Scheduled Task/Job	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	efb2f6452d7b0a63f6f2f4d8db49433259249df598391dd79f64df1ee3880a8d, a9aeb861817f3e4e74134622cbe298909e28d0fcc1e72f179a32adc637293a40, caa21a8f13a0b77ff5808ad7725ff3af9b74ce5b67426c84538b8fa43820a031, d37dc37fdcebbe0d265b8afad24198998ae8c3b2c6603a9258200ea8a1bd7b4a, 53e2dec3e16a0ff000a8c8c279eeeca8b4437edb8ec8462bfbd9f64ded8072d9, 827f7178802b2e92988d7cff349648f334bc86317b0b628f4bb9264285fccf5f, ee80f3e3ad43a283cbc83992e235e4c1b03ff3437c880be02ab1d15d92a8348a, de09ec092b11a1396613846f6b082e1e1ee16ea270c895ec6e4f553a13716304, d065623a7d943c6e5a20ca9667aa3c41e639e153600e26ca0af5d7c643384670, c08dd490860b54ae20fa9090274da9ffa1ba163f00d1e462e913cf8c68c11ac1

References

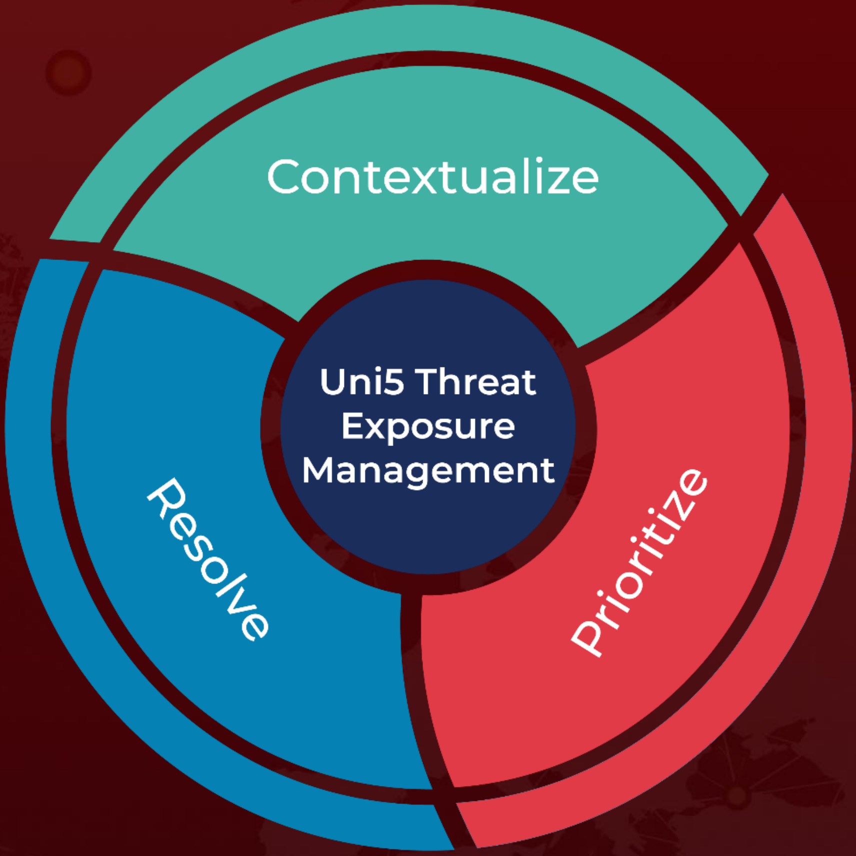
https://www.microsoft.com/en-us/security/blog/2025/08/27/storm-0501s-evolving-techniques-lead-to-cloud-based-ransomware/

https://cyble.com/threat-actor-profiles/storm-0501/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

August 29, 2025 • 7:30 AM

More at www.hivepro.com