INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-13 14:56 UTC

AI-Augmented Active Directory Enumeration and AWS Compromise Signal Speed-Over-Stealth Attacker Shift

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0658
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows Server (Active Directory), Amazon Web Services (AWS), S3, ECS, SQS, IAM
Published	2026-07-13T07:02:33
Discovery Source	Rss

Executive Summary

Two separate intrusions, reported by The Hacker News citing Sygnia research, document attackers using AI to accelerate familiar techniques rather than invent new ones, compressing attack timelines significantly. In the first incident, compromised credentials enabled RDP access followed by AI-assisted Active Directory enumeration and data exfiltration to cloud storage. In the second, an AWS environment spanning S3, ECS, SQS, and IAM was reportedly compromised within 72 hours via AI-assisted credential chaining. The primary business risk is speed: controls calibrated for human-paced attacks may not detect or contain intrusions that complete lateral movement and exfiltration within hours.

Technical Analysis

Two incidents, reported as separate intrusions with no confirmed attribution, illustrate AI functioning as an operational accelerant rather than a technique innovator. In the first, an unknown actor gained initial access via RDP (T1021.001) using compromised credentials (T1078) and executed a suspected AI-generated PowerShell script (T1059.001) to enumerate Active Directory accounts and permission groups (T1087.002, T1482, T1069). Exfiltration used s5cmd, a high-performance S3 transfer utility (T1530, T1567), and SharpShares for network share enumeration (T1135). In the second incident, documented by Sygnia, initial AWS access escalated to compromise of S3, ECS, SQS, and IAM within 72 hours. AI-assisted credential chaining (T1552.005) accelerated lateral movement and privilege escalation (T1098, T1136, T1078.004). Masquerading (T1036) and defense impairment (T1562) were also reported. Relevant weaknesses include CWE-200 (information exposure), CWE-269 (improper privilege management), and CWE-522 (insufficiently protected credentials). No

CVE identifiers are associated with these incidents. No patches are applicable; the attack surface is credential and configuration posture. Primary sourcing is The Hacker News referencing Sygnia research. Independent corroboration from CISA, NVD, or affected-party advisories was not present in the source set at time of writing.

Action Checklist

1. Step 1: Containment, Audit all privileged Active Directory accounts and AWS IAM roles for unauthorized access or recent changes. Rotate credentials for any account that accessed systems via RDP in the past 30 days, prioritizing service accounts and administrator accounts. Revoke or restrict any AWS IAM role with cross-service access to S3, ECS, SQS, and IAM simultaneously (NIST AC-2, NIST AC-6, CIS 5.1).
2. Step 2: Detection, Review Windows Security Event logs for Event ID 4624 (RDP logon), 4688 (process creation with PowerShell), and 4662/4661 (AD object enumeration). In AWS CloudTrail, query for ListBuckets, GetObject, CreateUser, AttachRolePolicy, and RunTask API calls, especially sequences where a single identity touches S3, ECS, SQS, and IAM within a short window. Look for s5cmd and SharpShares execution artifacts in EDR telemetry and Windows process creation logs (NIST AU-2, NIST AU-6, CIS 8.2).
3. Step 3: Eradication, Enforce MFA on all RDP-accessible accounts and all AWS IAM users and roles with console or programmatic access (CIS 6.3, CIS 6.4, CIS 6.5, D3-MFA). Remove or restrict PowerShell execution policy where full access is not operationally required. Enumerate and remove any accounts or IAM roles created during the suspected intrusion window (NIST AC-2, NIST IR-4).
4. Step 4: Recovery, Validate that all newly created or modified IAM roles, policies, and AD accounts have been reviewed and remediated. Enable AWS CloudTrail in all regions if not already active and confirm log integrity. Confirm s5cmd and SharpShares are not present in enterprise software inventory (CIS 2.1, CIS 2.3). Monitor AD and AWS IAM for 30 days post-remediation for recurrence (NIST AU-6, NIST SI-4).
5. Step 5: Post-Incident, Assess detection gap: if AI-generated scripts bypassed existing endpoint controls, evaluate whether behavioral detection rules cover PowerShell obfuscation and unusual AD query patterns. Review cloud IAM privilege scope against least-privilege baseline (NIST AC-6, CIS 5.4). Document timeline compression observed in the AWS incident as a planning input for incident response playbook SLAs, 72-hour full compromise requires detection and containment capabilities well inside that window (D3-LAM, D3-UAP, D3-CRO).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive stakeholders immediately if CloudTrail evidence confirms data was exfiltrated from S3 buckets containing PII, PHI, or regulated financial data, or if IAM role compromise affected production ECS workloads, triggering breach notification obligations under GDPR, HIPAA, or applicable state data protection laws.

Recovery Notes	Post-containment, validate all IAM roles and AD accounts against a pre-incident baseline snapshot before restoring any service dependencies; pay particular attention to ECS task definitions and SQS queue policies that may have been silently modified by attacker-created IAM roles during the 72-hour compromise window. Monitor AWS CloudTrail and AD Security Event Logs continuously for 30 days, with specific alerting on the API call sequence (CreateUser → AttachRolePolicy → RunTask) and AD enumeration Event IDs (4661/4662) at velocities exceeding normal operational baselines. Given the AI-assisted timeline compression documented in the Sygnia research, any recurrence indicators must trigger immediate containment without waiting for full triage — the standard 24–48-hour analysis window is incompatible with an adversary capable of full AWS environment compromise in 72 hours.
Forensic Artifacts	Windows Security Event Log entries for Event IDs 4624 (Logon Type 10 — RDP), 4661/4662 (AD object access with high-velocity LDAP filter patterns consistent with AI-generated enumeration), and 4688 (process creation for s5cmd.exe and SharpShares.exe) on domain controllers and RDP-accessible hosts | AWS CloudTrail logs capturing the cross-service API sequence (ListBuckets, GetObject, CreateUser, AttachRolePolicy, RunTask) attributed to a single principal identity within a compressed timeframe, stored in 'CloudTrail/AWSLogs//CloudTrail//' | PowerShell Script Block Logging output (Event ID 4104) from RDP-accessed hosts containing AI-generated AD enumeration scripts — identifiable by automated LDAP filter construction, high query density, and structured output formatting atypical of human-authored scripts | Windows Prefetch files at 'C:\Windows\Prefetch\S5CMD*.pf' and 'SHARPHARES*.pf' confirming execution of the specific data exfiltration and AD enumeration tools named in the Sygnia campaign report | RAM image from compromised hosts and domain controllers capturing in-memory Kerberos tickets, live LDAP query handles, and any fileless AI-generated script payloads that executed without writing to disk — volatile and unrecoverable after session termination or system reboot

Per-Action IR Details

Step 1: Containment — Audit all privileged Active Directory accounts and AWS IAM roles for unauthorized access or recent changes. Rotate credentials for any account that accessed systems via RDP in the past 30 days, prioritizing service accounts and administrator accounts. Revoke or scope-down any AWS IAM role with cross-service access to S3, ECS, SQS, and IAM simultaneously (NIST AC-2, NIST AC-6, CIS 5.1).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Run 'Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,MemberOf | Where-Object {$_.LastLogonDate -gt (Get-Date).AddDays(-30)} | Select Name,LastLogonDate,PasswordLastSet' to enumerate recently active AD accounts. For AWS, use the AWS CLI: 'aws iam generate-credential-report && aws iam get-credential-report' to identify IAM users with active access keys and recent console logins. Use 'aws iam list-attached-role-policies --role-name ' to map cross-service permissions for any role touching S3, ECS, SQS, and IAM simultaneously.

Evidence: BEFORE rotating any credential or revoking any AWS session token, capture: (1) Active RDP sessions via 'query session /server:' and Windows Security Event Log Event ID 4624 (Logon Type 10) filtered to the last 30 days; (2) In-memory Kerberos tickets via Mimikatz 'sekurlsa::tickets /export' or Volatility 'kerberos' plugin on a RAM image of the affected DC or workstation — AI-assisted AD enumeration tools may leave ticket artifacts; (3) AWS IAM credential report and 'aws sts get-caller-identity' for any active programmatic sessions; (4) 'aws cloudtrail lookup-events --lookup-attributes AttributeKey=Username,AttributeValue=' output covering the 30-day window to capture the full sequence of cross-service API calls before token revocation destroys session context.

Step 2: Detection — Review Windows Security Event logs for Event ID 4624 (RDP logon), 4688 (process creation with PowerShell), and 4662/4661 (AD object enumeration). In AWS CloudTrail, query for ListBuckets, GetObject, CreateUser, AttachRolePolicy, and RunTask API calls — especially sequences where a single identity touches S3, ECS, SQS, and IAM within a short window. Look for s5cmd and SharpShares execution artifacts in EDR telemetry and Windows process creation logs (NIST AU-2, NIST AU-6, CIS 8.2).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (Process Create) for s5cmd.exe and SharpShares.exe by hash and image name. Use this PowerShell query against Windows Security logs: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4688,4661,4662)} | Select TimeCreated,Id,Message | Export-Csv ad_enum_review.csv'. For AWS without a SIEM, use CloudTrail Insights (free tier) or run: 'aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=CreateUser' and repeat for AttachRolePolicy and RunTask, then manually correlate timestamps to identify the same principal touching all four services within a 72-hour window.

Evidence: The following volatile artifacts must be captured before any containment action: (1) Live process list on RDP-accessed hosts via 'Get-Process | Select Name,Id,Path,StartTime' — AI-generated enumeration scripts may be running as ephemeral PowerShell child processes; (2) Active network connections via 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' to identify live exfiltration channels to cloud storage endpoints consistent with s5cmd transfers; (3) PowerShell command history at '%APPDATA%\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt' on the RDP-accessed host — AI-generated scripts will produce anomalous, high-density AD LDAP queries not typical of human operators; (4) Windows prefetch files at 'C:\Windows\Prefetch\S5CMD*.pf' and 'SHARPHARES*.pf' confirming tool execution prior to log review; (5) CloudTrail event history export for the 72-hour window preceding detection, before any IAM changes could alter the event source identity chain.

Step 3: Eradication — Enforce MFA on all RDP-accessible accounts and all AWS IAM users and roles with console or programmatic access (CIS 6.3, CIS 6.4, CIS 6.5, D3-MFA). Remove or restrict PowerShell execution policy where full access is not operationally required. Enumerate and remove any accounts or IAM roles created during the suspected intrusion window (NIST AC-2, NIST IR-4).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Use Group Policy to enforce PowerShell Constrained Language Mode on non-admin hosts: set 'HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Environment__PSLockdownPolicy' to '4'. Enumerate IAM accounts created during the intrusion window with: 'aws iam list-users --query "Users[?CreateDate>=\"\"]"' and 'aws iam list-roles --query "Roles[?CreateDate>=\"\"]"'. For MFA enforcement on RDP, configure Network Level Authentication (NLA) via Group Policy under 'Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services' and pair with Azure AD Conditional Access or Duo free tier for MFA without enterprise licensing.

Evidence: BEFORE removing any IAM role or AD account created during the intrusion, and before modifying PowerShell execution policy on compromised hosts, capture: (1) Full memory image of any host where AI-generated enumeration scripts executed — these scripts may reside only in memory or in PowerShell's in-memory runspace with no on-disk artifact; (2) 'aws iam list-roles', 'aws iam list-users', and 'aws iam list-policies --scope Local' output to establish a complete pre-remediation snapshot of the IAM state the attacker built; (3) Windows Registry export of 'HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' on RDP-accessed hosts for persistence mechanisms; (4) SharpShares and s5cmd artifacts — specifically '%TEMP%*.exe', '%USERPROFILE%\Downloads*.exe', and any

LDAP query logs in Wireshark captures on the DC network interface — before policy changes alter execution context.

Step 4: Recovery — Validate that all newly created or modified IAM roles, policies, and AD accounts have been reviewed and remediated. Enable AWS CloudTrail in all regions if not already active and confirm log integrity. Confirm s5cmd and SharpShares are not present in enterprise software inventory (CIS 2.1, CIS 2.3). Monitor AD and AWS IAM for 30 days post-remediation for recurrence (NIST AU-6, NIST SI-4).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.3 (Address Unauthorized Software), CIS 8.2 (Collect Audit Logs)

Compensating: Enable multi-region CloudTrail with log file validation via: 'aws cloudtrail create-trail --name org-trail --s3-bucket-name --is-multi-region-trail --enable-log-file-validation'. Validate CloudTrail log integrity with: 'aws cloudtrail validate-logs --trail-arn --start-time '. For software inventory on Windows endpoints, run: 'Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Select DisplayName,InstallDate | Where-Object {$_.DisplayName -match "s5cmd|SharpShares"}' and scan all host prefetch directories for 'S5CMD*.pf'. Deploy osquery with a query targeting 'SELECT name, path, pid FROM processes WHERE name IN ("s5cmd.exe","SharpShares.exe")' for ongoing monitoring.

Evidence: Before declaring recovery complete and restoring any isolated systems to production, verify: (1) CloudTrail log integrity hash validation passes for the full intrusion window — attacker-created IAM users with CloudTrail write access could have tampered with logs via 'DeleteTrail' or 'StopLogging' API calls; confirm no such events appear in CloudTrail itself; (2) AD replication metadata via 'repadmin /showchanges /cookie:' to identify any schema or object changes made during the AI-assisted enumeration phase that may persist post-account removal; (3) S3 bucket access logs and server-side encryption status on all buckets accessible to the compromised roles to confirm no exfiltrated data remains in attacker-controlled staging locations; (4) Confirm ECS task definitions were not modified to include backdoor container images by reviewing 'aws ecs list-task-definitions' and diffing against last known-good configuration.

Step 5: Post-Incident — Assess detection gap: if AI-generated scripts bypassed existing endpoint controls, evaluate whether behavioral detection rules cover PowerShell obfuscation and unusual AD query patterns. Review cloud IAM privilege scope against least-privilege baseline (NIST AC-6, CIS 5.4). Document timeline compression observed in the AWS incident as a planning input for incident response playbook SLAs — 72-hour full compromise requires detection and containment capabilities well inside that window (D3-LAM, D3-UAP, D3-CRO).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Develop Sigma rules targeting AI-generated AD enumeration patterns: unusually high-velocity LDAP queries (Event ID 4662 with Object Type 'organizationalUnit' or 'group' firing >100 times in 60 seconds from a single source IP) and PowerShell processes spawning child processes with Base64-encoded command lines (Event ID 4688, CommandLine contains '-EncodedCommand'). Use the free Sigma converter to deploy to Windows Event Forwarding. For IAM least-privilege assessment, run AWS IAM Access Analyzer (free, native) to identify roles with unused cross-service permissions across S3, ECS, SQS, and IAM — the specific combination exploited in this campaign. Update IR playbook SLAs to mandate initial triage within 4 hours and containment decisions within 24 hours, given the documented 72-hour full-compromise timeline.

Evidence: Post-incident forensic review should prioritize: (1) Complete PowerShell Script Block Logging output (Event ID 4104) from all hosts accessed via RDP during the intrusion — AI-generated scripts produce structurally distinctive patterns (repetitive enumeration loops, automated LDAP filter construction) that can be used to build detection signatures; (2) CloudTrail sequence reconstruction of the full API call chain from initial credential use through IAM privilege escalation to cross-service data access — this documents the AI-accelerated attack tempo for playbook SLA calibration; (3) AWS IAM Access Advisor data ('aws iam generate-service-last-accessed-details') for all roles involved, to establish which cross-service permissions were actually used versus granted, informing the least-privilege

remediation baseline.

Detection Guidance

Active Directory environment: Enable and review Windows Security Event ID 4624 (logon type 10 = RDP), 4688 (PowerShell spawned from unusual parent), 4662/4661 (directory service access), and 4776 (credential validation). Alert on PowerShell executions that query LDAP or invoke net group, Get-ADUser, or Get-ADGroupMember at volume. Look for SharpShares execution artifacts (process name, hash, or command-line pattern) in EDR telemetry. Flag s5cmd process execution anywhere outside authorized data pipeline infrastructure. AWS environment: Query CloudTrail for the following API call sequences from a single identity within any 6-hour window, ListBuckets or GetObject, followed by RunTask or CreateService (ECS), followed by SendMessage (SQS), followed by CreateUser, AttachUserPolicy, or CreateAccessKey (IAM). Alert on any IAM policy attachment granting AdministratorAccess or wildcard S3 access outside a change-management window. Enable GuardDuty findings for CredentialAccess and Exfiltration categories. Behavioral indicators include: According to Sygnia research, AI-generated PowerShell scripts tend toward syntactically clean, well-commented code executing sensitive operations; this pattern combined with unusual execution context (non-admin user, off-hours, new device) is a meaningful signal. Attribution remains unknown; threat actor infrastructure IOCs are not available from current sources.

Framework Mappings

MITRE-ATTACK

- **T1530** — Data from Cloud Storage
- **T1087.002** — Domain Account
- **T1136** — Create Account
- **T1021.001** — Remote Desktop Protocol
- **T1036** — Masquerading
- **T1552.005** — Cloud Instance Metadata API
- **T1098** — Account Manipulation
- **T1059.001** — PowerShell
- **T1135** — Network Share Discovery
- **T1482** — Domain Trust Discovery
- **T1069** — Permission Groups Discovery
- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1078.004** — Cloud Accounts
- **T1560** — Archive Collected Data
- **T1087** — Account Discovery
- **T1041** — Exfiltration Over C2 Channel
- **T1562** — Impair Defenses

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents
- **CC6.3** — Authorizes, modifies, or removes access

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection
T1087.002	Domain Account	Discovery
T1136	Create Account	Persistence
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1036	Masquerading	Defense-Evasion
T1552.005	Cloud Instance Metadata API	Credential-Access
T1098	Account Manipulation	Persistence
T1059.001	PowerShell	Execution
T1135	Network Share Discovery	Discovery
T1482	Domain Trust Discovery	Discovery
T1069	Permission Groups Discovery	Discovery
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion
T1560	Archive Collected Data	Collection
T1087	Account Discovery	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration
T1562	Impair Defenses	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/07/attacker-uses-suspected-ai-genera...	T2
Securely extend and access on-premises Active Directory domain ...	https://aws.amazon.com/blogs/security/securely-extend-and-access-on...	T3

Source	URL	Tier
Amazon Web Services provider permissions - Administrator Guide	https://docs-cortex.paloaltonetworks.com/r/Cortex-CLOUD/Cortex-Clou...	**T1**
AWS Directory Service	https://aws.amazon.com/directoryservice/	**T3**

Generated 2026-07-13 14:56 UTC by TJS Security Command Center