INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-28 13:44 UTC

UNC6692 Exploits Microsoft Teams Social Engineering and AWS S3 Abuse in Targeted Intrusion Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0233
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Teams (external tenant communication feature), Amazon Web Services S3 (bucket infrastructure abuse); enterprise environments using both platforms
Published	2026-04-27T16:12:34
Discovery Source	Rss

Executive Summary

UNC6692, a newly identified threat actor, is conducting targeted intrusion campaigns that abuse Microsoft Teams cross-tenant messaging to deliver malware and leverage AWS S3 buckets for command-and-control infrastructure. Enterprises using both platforms are at risk of initial compromise through social engineering attacks that exploit the inherent trust employees place in internal communication tools. The business risk includes unauthorized network access, data exfiltration, and potential lateral movement, compounded by detection difficulty due to malicious traffic blending with legitimate cloud services.

Technical Analysis

UNC6692 conducts multi-stage intrusions beginning with Microsoft Teams social engineering, specifically abusing external tenant communication to deliver or lure execution of a custom malware family designated 'Snow' (T1566.004, T1204.002, T1204.001). AWS S3 buckets are abused for payload staging and C2 communications, blending malicious egress with legitimate cloud traffic (T1567.002, T1608.002, T1583.006, T1102). The campaign abuses trusted cloud services (Microsoft Teams, AWS S3) to evade detection controls. Relevant CWEs include CWE-693 (Protection Mechanism Failure, Teams external messaging trust abuse) and CWE-1021 (Improper Restriction of Rendered UI Layers, UI deception in social engineering). MITRE ATT&CK techniques span initial access (T1598.004, Spearphishing via Teams), ingress tool transfer (T1105), valid account abuse (T1078), and application layer protocol communications (T1071.001). No CVE identifier has

been assigned; this is a configuration and trust-abuse campaign, not a software vulnerability exploit. Source confidence is medium, reporting originates from a single outlet (Dark Reading, T3); no corroboration from CISA, MITRE, or NIST has been confirmed as of this writing.

Action Checklist

1. Containment: Restrict or disable Microsoft Teams external tenant communication (cross-tenant access) for user populations that do not require it. In Microsoft Entra ID, review and tighten Cross-Tenant Access Settings under External Identities to block inbound messaging from unknown or unvetted tenants. Identify any S3 buckets in your AWS environment that were recently created or modified and verify their intended purpose.
2. Detection: Review Microsoft Teams audit logs (via Microsoft Purview or Defender for Office 365) for messages received from external tenants containing file attachments, URLs, or requests to execute files. In AWS CloudTrail, search for anomalous S3 API calls (GetObject, PutObject) from internal hosts, particularly to buckets not provisioned by your team. Hunt for the 'Snow' malware family in endpoint telemetry; query EDR platforms for unsigned executables launched from Teams-associated process trees (Teams.exe, Update.exe) or downloads via S3 presigned URLs.
3. Eradication: Remove any unauthorized S3 buckets or bucket policies permitting public or cross-account access. Revoke compromised credentials identified via T1078 (valid account abuse). Isolate and reimage any endpoints where Snow malware indicators are present. Rotate credentials for any accounts that interacted with suspicious Teams messages or S3 resources.
4. Recovery: After remediation, validate that Cross-Tenant Access Settings have been applied tenant-wide and are not overridden by per-user exceptions. Confirm CloudTrail logging is enabled on all S3 buckets (data events, not just management events). Re-enable production operations only after endpoint scans return clean and no anomalous C2 traffic to S3 endpoints is observed in network logs.
5. Post-Incident: Conduct a review of Teams external communication policies and determine whether the business requires cross-tenant messaging at current permissiveness levels. Implement S3 guardrails via AWS Service Control Policies (SCPs) to restrict bucket creation and public access. Map control gaps to NIST CSF PR.AC (Access Control) and DE.CM (Continuous Monitoring). Add Teams social engineering scenarios to security awareness training.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to CISO and legal counsel immediately if Snow malware indicators are confirmed on any endpoint with access to PII, PHI, or financial data, if any AWS IAM role with cross-account or administrative privileges authenticated to attacker-controlled S3 buckets (potential data exfiltration triggering breach notification obligations), or if the security team lacks the tooling or capacity to complete containment and eradication within 24 hours of incident declaration.

Recovery Notes	After containment and eradication, monitor all endpoints in the blast radius for at least 14 days using Sysmon Event ID 3 (NetworkConnect) and Event ID 1 (ProcessCreate) for Snow malware re-execution or C2 re-establishment to *.s3.amazonaws.com endpoints. Validate that no Teams external tenant exceptions were re-enabled by end users or administrators by running `Get-MgPolicyCrossTenantAccessPolicyPartner` weekly for the first 30 days post-recovery. Do not return any endpoint to production without a clean YARA scan using a Snow-malware-specific rule set and confirmation that the endpoint's process ancestry for Teams.exe shows no unsigned child processes in the prior 72 hours.
Forensic Artifacts	Microsoft Purview Unified Audit Log — Teams message events (RecordType: MicrosoftTeams, Operation: MessageSent/FileSent) filtered on ExternalAccess=true, preserving sender TenantId and attachment SHA256; these records document UNC6692's initial delivery mechanism and the specific external tenant IDs used in the campaign. | AWS CloudTrail S3 data events (GetObject, PutObject, DeleteObject) — must be data-plane events, not management events; filter on sourceIPAddress matching internal RFC-1918 ranges to identify internal hosts beaconing to UNC6692-controlled S3 buckets and any data staged for exfiltration. | Windows endpoint file system artifacts — `%LocalAppData%\Microsoft\Teams\Downloads\` and `%USERPROFILE%\Downloads\` for Snow malware dropper files delivered via Teams; collect SHA256 hashes, file metadata (created/modified timestamps), and Zone.Identifier alternate data streams to confirm S3 presigned URL as the download source. | Sysmon Event ID 1 (ProcessCreate) and Event ID 3 (NetworkConnect) — filter on ParentImage containing Teams.exe or Update.exe with child processes that are unsigned executables, and outbound TLS connections to *.s3.amazonaws.com from non-browser process names; this artifact chain documents the Snow malware execution and C2 communication path specific to UNC6692's delivery method. | Windows Registry run key exports — `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` plus `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce` collected via `reg export` before reimaging; Snow malware families commonly establish persistence here after initial execution from Teams-delivered payloads.

Per-Action IR Details

Containment — Restrict or disable Microsoft Teams external tenant communication (cross-tenant access) for user populations that do not require it. In Microsoft Entra ID, review and tighten Cross-Tenant Access Settings under External Identities to block inbound messaging from unknown or unvetted tenants. Identify any S3 buckets in your AWS environment that were recently created or modified and verify their intended purpose.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Choose a containment strategy based on the type of incident; isolate affected systems and block attacker communication channels before eradication begins.

Controls: NIST IR-4 (Incident Handling) — implement containment as part of the documented incident handling capability, NIST AC-17 (Remote Access) — restrict external tenant communication pathways that UNC6692 exploits for initial access, NIST SC-7 (Boundary Protection) — enforce boundary controls on Microsoft Entra ID Cross-Tenant Access Settings to deny inbound messaging from unvetted external tenants, CIS 4.4 (Implement and Manage a Firewall on Servers) — block outbound S3 presigned URL traffic at the perimeter to sever active C2 channels to UNC6692-controlled buckets, CIS 6.2 (Establish an Access Revoking Process) — immediately revoke or restrict Teams external access permissions for user accounts that do not have a documented cross-tenant business need

Compensating: Without enterprise tooling: (1) Use the Microsoft Entra ID portal directly — navigate to External Identities > Cross-tenant access settings, add a blanket inbound block for 'All external organizations,' then create

explicit allow-list exceptions for vetted partner tenants only. Export the current settings first via: `Get-MgPolicyCrossTenantAccessPolicy | ConvertTo-Json -Depth 10 > crosstenantpolicy_baseline.json`. (2) For AWS S3 exposure, run `aws s3api list-buckets --query 'Buckets[*].[Name,CreationDate]' --output table` and follow with `aws s3api get-bucket-acl --bucket ` and `aws s3api get-bucket-policy --bucket ` for each bucket created or modified in the last 30 days. Flag any bucket with public ACLs or cross-account trust policies not in your CMDB.

Evidence: BEFORE modifying Entra ID settings, export the current Cross-Tenant Access Policy baseline (see compensating control command above) to document attacker-permissive configurations as evidence. From AWS CloudTrail, extract the full S3 API event history for the suspicious buckets: `aws cloudtrail lookup-events --lookup-attributes AttributeKey=ResourceName,AttributeValue= --output json > s3_cloudtrail_events.json`. Capture Teams message metadata (sender tenant ID, external user UPN, message timestamp, attachment SHA256) from Microsoft Purview Audit before any policy change purges the activity log. Preserve network flow logs showing internal host connections to S3 endpoints (*.s3.amazonaws.com) on ports 443/80 as evidence of C2 beacon activity.

Detection — Review Microsoft Teams audit logs (via Microsoft Purview or Defender for Office 365) for messages received from external tenants containing file attachments, URLs, or requests to execute files. In AWS CloudTrail, search for anomalous S3 API calls (GetObject, PutObject) from internal hosts, particularly to buckets not provisioned by your team. Hunt for the 'Snow' malware family in endpoint telemetry; query EDR platforms for unsigned executables launched from Teams-associated process trees (Teams.exe, Update.exe) or downloads via S3 presigned URLs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Analyze indicators of compromise from multiple log sources, correlate events across platforms, and prioritize incidents based on functional impact and scope of compromise.

Controls: NIST IR-4 (Incident Handling) — execute detection and analysis phase of the incident handling capability against UNC6692 TTPs, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review Microsoft Purview and CloudTrail audit records for indicators specific to UNC6692 cross-tenant message delivery and S3 C2 patterns, NIST SI-4 (System Monitoring) — monitor endpoint process trees for Snow malware execution chains originating from Teams.exe and Update.exe parent processes, NIST AU-2 (Event Logging) — verify that Teams message audit events and AWS S3 data-plane events (GetObject, PutObject) are captured at sufficient granularity to support this hunt, CIS 8.2 (Collect Audit Logs) — confirm audit logs are enabled and centrally collected for Microsoft 365 unified audit log and AWS CloudTrail before hunting begins

Compensating: Without EDR: (1) Deploy Sysmon with SwiftOnSecurity config; add a targeted rule capturing ProcessCreate events where ParentImage contains 'Teams.exe' or 'Update.exe' and Image is not in an approved allowlist — log to Windows Event ID 1. (2) Hunt Snow malware execution artifacts via PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'Teams|Update.exe'} | Select-Object TimeCreated, Message | Export-Csv teams_process_hunt.csv`. (3) For AWS without a SIEM, use AWS CLI Athena queries against CloudTrail Lake or manually filter: `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventName,AttributeValue=GetObject --start-time 2025-01-01 --output json | python3 -c "import sys,json; [print(e) for e in json.load(sys.stdin)['Events'] if 's3.amazonaws.com' in str(e)]"`. (4) Use a Sigma rule converted to grep against exported CloudTrail JSON to flag GetObject calls from internal RFC-1918 source IPs to unknown bucket names.

Evidence: Query Microsoft Purview Audit (Operations: MessageSent, FileSent, MeetingParticipantDetail) filtering on RecordType 'MicrosoftTeams' and ExternalAccess eq 'true'; export to CSV preserving sender TenantId, recipient UPN, attachment name, and SHA256. From AWS CloudTrail, pull all S3 data events (must be explicitly enabled — management events alone do NOT capture GetObject/PutObject) for the past 90 days filtering on sourceIPAddress matching internal RFC-1918 ranges. On compromised endpoints, collect: (a) `%LocalAppData%\Microsoft\Teams\` download cache for dropped payloads, (b) Prefetch files (`C:\Windows\Prefetch\`) for Snow malware executable names, (c) Sysmon Event ID 3 (NetworkConnect) records showing outbound TLS connections to *.s3.amazonaws.com from non-browser processes, (d) Windows Security Event ID 4688 (Process Creation) showing unsigned executables with no publisher certificate spawned under Teams process ancestry.

Eradication — Remove any unauthorized S3 buckets or bucket policies permitting public or cross-account access. Revoke compromised credentials identified via T1078 (valid account abuse). Isolate and reimage any endpoints where Snow malware indicators are present. Rotate credentials for any accounts that interacted with suspicious Teams messages or S3 resources.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: Eliminate the components of the incident, such as deleting malware, disabling breached user accounts, and removing attacker-planted persistence mechanisms, after all affected hosts are identified.

Controls: NIST IR-4 (Incident Handling) — execute eradication activities as part of the incident handling lifecycle, ensuring all UNC6692 footholds are removed before recovery, NIST SI-2 (Flaw Remediation) — remove Snow malware and any persistence mechanisms (scheduled tasks, registry run keys) planted via Teams-delivered payloads, NIST SI-3 (Malicious Code Protection) — scan reimaged and neighboring endpoints for Snow malware family indicators before returning to production, NIST AC-2 (Account Management) — disable and rotate credentials for all accounts that received UNC6692 Teams messages or whose tokens were used to authenticate to attacker-controlled S3 buckets (MITRE ATT&CK T1078 — Valid Accounts), CIS 5.3 (Disable Dormant Accounts) — disable any accounts identified as compromised or dormant that UNC6692 may have leveraged for persistence via T1078, CIS 7.2 (Establish and Maintain a Remediation Process) — execute credential rotation and bucket removal against a risk-prioritized list, starting with accounts with admin or S3 write privileges

Compensating: Without enterprise tooling: (1) Delete attacker S3 infrastructure using `aws s3 rb s3:// --force` after preserving bucket contents as evidence; remove permissive bucket policies with `aws s3api delete-bucket-policy --bucket `. (2) Revoke all active AWS IAM sessions for compromised identities: `aws iam delete-access-key --access-key-id --user-name ` and `aws sts get-caller-identity` to verify. (3) For Microsoft 365, revoke all active refresh tokens for affected accounts using: `Revoke-MgUserSignInSession -UserId ` (Microsoft Graph PowerShell). (4) On endpoints, before reimaging collect a full memory image with Magnet RAM Capture or WinPmem for Snow malware analysis, then wipe and reimage from a known-good baseline. (5) Create a YARA rule targeting Snow malware family characteristics and scan remaining endpoints with ClamAV or standalone YARA binary before returning them to production.

Evidence: BEFORE eradicating, capture: (a) Full memory dump of compromised endpoints using WinPmem (`winpmem_mini_x64.exe output.raw`) to preserve in-memory Snow malware artifacts, injected code, and decrypted C2 configuration; (b) Copy of the malicious Teams attachment from `%LocalAppData%\Microsoft\Teams\Downloads\` or the user's Downloads folder with SHA256 hash documented; (c) Registry export of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` to document any Snow malware persistence keys; (d) AWS IAM Access Advisor export for compromised accounts (`aws iam generate-service-last-accessed-details`) to determine the full scope of services accessed using stolen credentials; (e) Scheduled task export (`schtasks /query /fo LIST /v > scheduled_tasks_evidence.txt`) to capture any UNC6692-planted persistence mechanisms.

Recovery — After remediation, validate that Cross-Tenant Access Settings have been applied tenant-wide and are not overridden by per-user exceptions. Confirm CloudTrail logging is enabled on all S3 buckets (data events, not just management events). Re-enable production operations only after endpoint scans return clean and no anomalous C2 traffic to S3 endpoints is observed in network logs.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore systems to normal operation, confirm systems are functioning normally, and implement additional monitoring to watch for a recurrence of the attack before declaring the incident closed.

Controls: NIST IR-4 (Incident Handling) — execute recovery phase activities including verification of restored controls and enhanced monitoring for UNC6692 re-entry attempts, NIST AU-2 (Event Logging) — verify that AWS CloudTrail S3 data events (GetObject, PutObject, DeleteObject) are enabled on all production buckets, not just management events, to close the detection gap UNC6692 exploited, NIST AU-4 (Audit Storage Capacity) — ensure CloudTrail and Microsoft Purview log retention is sufficient (minimum 90 days recommended) to support retrospective hunting for UNC6692 activity predating incident declaration, NIST SI-7 (Software, Firmware, and Information Integrity) — validate

endpoint integrity via clean antivirus/YARA scan results before returning reimaged systems to production, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) — verify that firewall rules blocking outbound traffic to attacker S3 endpoints are in place and logged before resuming production, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — document the Cross-Tenant Access configuration state as a new security baseline and schedule recurring reviews

Compensating: Without enterprise tooling: (1) Validate Cross-Tenant Access policy tenant-wide using: `Get-MgPolicyCrossTenantAccessPolicy | ConvertTo-Json -Depth 10` and compare against the pre-incident baseline export to confirm no per-user overrides exist (check `Get-MgPolicyCrossTenantAccessPolicyPartner` for any partner-specific exceptions). (2) Enable S3 data event logging via AWS CLI: `aws cloudtrail put-event-selectors --trail-name --event-selectors '[{"ReadWriteType":"All","IncludeManagementEvents":true,"DataResources":[{"Type":"AWS::S3::Object","Values":["arn:aws:s3:::"]}]}]'`. (3) Monitor for C2 re-establishment using Wireshark or `tcpdump -i eth0 -w s3_traffic.pcap 'host *.s3.amazonaws.com and not src '` on perimeter hosts for a minimum of 14 days post-recovery. (4) Use osquery to continuously verify no Teams-ancestry processes are making unexpected network connections: `SELECT p.name, p.path, pn.remote_address FROM processes p JOIN process_open_sockets pn USING (pid) WHERE p.parent IN (SELECT pid FROM processes WHERE name = 'Teams.exe');`

Evidence: Before declaring recovery complete, collect and retain: (a) Screenshot and JSON export of the final Entra ID Cross-Tenant Access Settings configuration as the new approved baseline; (b) AWS Config snapshot confirming S3 bucket public access block is enabled on all buckets (`aws s3control get-public-access-block --account-id `); (c) 14-day network traffic summary from perimeter logs or Wireshark captures showing zero outbound connections to *.s3.amazonaws.com from endpoints or servers outside approved application IPs; (d) Clean YARA scan output from all endpoints in the blast radius, documenting the Snow malware rule set used and scan timestamp; (e) Microsoft Secure Score delta (pre- and post-incident) to document control improvement for the post-incident report.

Post-Incident — Conduct a review of Teams external communication policies and determine whether the business requires cross-tenant messaging at current permissiveness levels. Implement S3 guardrails via AWS Service Control Policies (SCPs) to restrict bucket creation and public access. Map control gaps to NIST CSF PR.AC (Access Control) and DE.CM (Continuous Monitoring). Add Teams social engineering scenarios to security awareness training.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Hold a lessons-learned meeting, produce an incident report, and identify systemic control gaps. Improvements should be implemented before the next incident occurs, not during it.

Controls: NIST IR-4 (Incident Handling) — update the incident handling capability based on lessons learned from the UNC6692 campaign, specifically for social-engineering-delivered malware via trusted communication platforms, NIST IR-8 (Incident Response Plan) — revise the incident response plan to include a playbook section for Teams-based social engineering and S3 C2 abuse, incorporating UNC6692 TTPs, NIST IR-2 (Incident Response Training) — add UNC6692-style Teams social engineering to the security awareness training curriculum, including specific red flags: external tenant sender badges, unsolicited file share links, and requests to execute downloaded files, NIST SI-5 (Security Alerts, Advisories, and Directives) — document UNC6692 campaign indicators as an internal advisory and distribute to security and IT operations teams for ongoing awareness, NIST RA-3 (Risk Assessment) — re-assess the risk of Microsoft Teams cross-tenant access and AWS S3 public bucket permissions in light of confirmed UNC6692 exploitation of these configurations, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate SCP-based S3 guardrails and Entra ID cross-tenant access restrictions into the organization's secure configuration baseline, CIS 6.3 (Require MFA for Externally-Exposed Applications) — validate MFA enforcement on all Microsoft 365 accounts as a structural control against the T1078 credential abuse UNC6692 used post-initial-access

Compensating: Without enterprise GRC tooling: (1) Draft AWS SCPs using the AWS-managed policy `AWS-DenyPublicS3Access` and attach to the root OU in AWS Organizations: `aws organizations create-policy --type SERVICE_CONTROL_POLICY --name DenyPublicS3 --description 'Block public S3 access org-wide' --content file://deny_public_s3_scp.json`. Use the AWS SCP example that denies `s3:PutBucketAcl` with `s3:x-amz-acl: public-read` or `public-read-write`. (2) For Teams social engineering training, create a tabletop exercise scenario using a real UNC6692 lure template: external Teams contact posing as a vendor, sending a OneDrive or S3 presigned URL to a 'contract document' that is actually a Snow malware dropper. Run this scenario with the IT and finance teams who are most likely to receive cross-tenant messages. (3) Map control gaps to NIST CSF 2.0 using the free CISA CSF 2.0

Reference Tool (no cost, no account required) and export the gap assessment as a one-page risk register entry.

Evidence: Post-incident documentation package must include: (a) Full timeline of UNC6692 activity from first malicious Teams message received to incident closure, sourced from Purview audit and CloudTrail timestamps; (b) Inventory of all external tenant IDs that sent messages to your organization in the 90 days prior to the incident (export from Purview: Operation = MessageSent, ExternalAccess = true); (c) List of all AWS S3 buckets that were publicly accessible or had cross-account trust policies at the time of the incident, with dates they were created and who created them (from CloudTrail CreateBucket events); (d) Before-and-after Entra ID Cross-Tenant Access policy JSON exports demonstrating the policy hardening applied; (e) Lessons-learned meeting notes documenting which NIST CSF PR.AC and DE.CM controls were absent or misconfigured that allowed UNC6692 to establish initial access and operate undetected.

Detection Guidance

Microsoft Teams: Query Microsoft Purview audit logs or Defender for Office 365 for ChatMessageReceived or FileShared events originating from external tenant domains not on an approved allowlist. Flag any external-tenant messages containing executable file types (.exe, .msi, .lnk, .bat, .ps1) or URLs pointing to S3 endpoints (*.s3.amazonaws.com, *.s3-*.amazonaws.com). AWS CloudTrail: Enable S3 data event logging if not already active. Alert on GetObject or PutObject API calls from internal hostnames to S3 buckets not provisioned by your cloud team, particularly calls using presigned URLs or anonymous access patterns. Network: Watch for outbound HTTP/HTTPS connections to *.s3.amazonaws.com from endpoints that are not cloud workloads; Teams client machines making repeated S3 egress calls are anomalous. Endpoint: Hunt for process execution chains originating from Teams.exe or its update process. Specifically, flag child processes that are unsigned, launched from the user's AppData or Temp directories, or that make outbound network calls to cloud storage endpoints. The Snow malware family has no publicly confirmed hashes as of this writing, behavioral detection is the primary available method. Note: IOC-level indicators (hashes, IPs, domains) have not been confirmed from authoritative sources at this confidence level.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`*.s3.amazonaws.com`	AWS S3 endpoints abused for C2 and payload delivery — pattern indicator only, not a specific malicious domain; requires corroboration with anomalous access patterns	LOW

Framework Mappings

MITRE-ATTACK

- **T1105** — Ingress Tool Transfer
- **T1598.004** — Spearphishing Voice
- **T1608.002** — Upload Tool
- **T1566.004** — Spearphishing Voice
- **T1078** — Valid Accounts

- **T1567.002** — Exfiltration to Cloud Storage
- **T1102** — Web Service
- **T1071.001** — Web Protocols
- **T1204.002** — Malicious File
- **T1204.001** — Malicious Link
- **T1583.006** — Web Services

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1105	Ingress Tool Transfer	Command-And-Control
T1598.004	Spearphishing Voice	Reconnaissance
T1608.002	Upload Tool	Resource-Development
T1566.004	Spearphishing Voice	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1567.002	Exfiltration to Cloud Storage	Exfiltration
T1102	Web Service	Command-And-Control
T1071.001	Web Protocols	Command-And-Control

Technique ID	Technique Name	Tactic
T1204.002	Malicious File	Execution
T1204.001	Malicious Link	Execution
T1583.006	Web Services	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cloud-security/unc6692-social-engineeri...	T3
Google, Microsoft, Amazon AWS vuln disclosure failures - LinkedIn	https://www.linkedin.com/posts/jonathan-leitschuh_google-microsoft-...	T3
Breaking Down S3 Ransomware: Variants, Attack Paths and Trend ...	https://www.trendmicro.com/en_us/research/25/k/s3-ransomware.html	T3
AWS Falls Victim to Ransomware - Arete Incident Response	https://areteir.com/resources/codefinger-ransomware-encrypts-aws-s3...	T3
flAWS Level 1 and S3 Bucket Vulnerabilities - Kyle Topasna - Medium	https://kyletopasna.medium.com/flaws-level-1-and-s3-bucket-vulnerab...	T3

Generated 2026-04-28 13:44 UTC by TJS Security Command Center