INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-23 06:27 UTC

Nation-State Actors Weaponize ROADtools Against Entra ID: Device Registration, PRT Abuse, and MFA Bypass at Scale

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0353
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Entra ID (Azure Active Directory), Microsoft Azure, Microsoft Graph API, Azure Device Registration Service
Published	2026-05-22T10:00:24+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Three nation-state threat actors, APT29 (Midnight Blizzard), APT33 (Curious Serpens), and UTA0355, are actively exploiting the open-source ROADtools framework to compromise Microsoft Entra ID environments through rogue device registration and Primary Refresh Token (PRT) abuse. The attack achieves persistent, MFA-bypassing access to Microsoft cloud services using legitimate API calls, making it indistinguishable from normal administrative traffic. Any organization running Microsoft Entra ID without enforced Conditional Access policies requiring compliant devices is at risk of undetected, long-term identity compromise that can cascade across the entire Microsoft 365 and Azure estate.

Technical Analysis

APT29, APT33, and UTA0355 have operationalized ROADtools, a publicly available Entra ID enumeration and exploitation framework, to execute a multi-stage identity attack chain against Microsoft Entra ID (formerly Azure Active Directory). The attack does not exploit a single patched CVE; it abuses legitimate Microsoft APIs (Microsoft Graph API, Azure Device Registration Service) through the following techniques: (1) Unauthorized device registration (T1098.005) to obtain valid device credentials and join rogue devices to the tenant; (2) PRT theft and replay (T1550.001, T1550) to acquire persistent authenticated sessions that survive MFA enforcement, mapped to CWE-294 (Authentication Bypass by Capture-replay); (3) Token exchange manipulation to pivot laterally across Microsoft cloud services. CWE-287 (Improper Authentication) and CWE-522 (Insufficiently Protected Credentials) further describe the underlying weaknesses. MITRE techniques include T1528 (Steal

Application Access Token), T1556.006 (Modify Authentication Process: Multi-Factor Authentication), T1621 (Multi-Factor Authentication Request Generation), T1566.001 (Spearphishing Attachment) as an initial access vector, T1078/T1078.004 (Valid Accounts: Cloud Accounts), T1087 (Account Discovery), T1110.003 (Password Spraying), and T1098 (Account Manipulation). Because all API calls are structurally legitimate, signature-based detection and standard MFA controls are insufficient. Behavioral analytics on device registration events and token issuance patterns are required. No vendor patch resolves this campaign; hardening and detection engineering are the primary mitigations. Source: Unit 42 (Palo Alto Networks), Microsoft Entra documentation.

Action Checklist

1. Step 1: Immediate Containment, Audit all registered devices in Entra ID immediately. In the Azure portal, navigate to Entra ID > Devices > All Devices and filter for recently registered devices (last 30-90 days). Disable or remove any device not recognized in your asset inventory (CIS 1.1, Enterprise Asset Inventory, CIS 1.2, Address Unauthorized Assets). Restrict device registration permissions to authorized users only via Entra ID device settings (Users may register their devices: set to 'Selected' or 'None' unless operationally required).
2. Step 2: Detection, Enable and query Entra ID Sign-In Logs and Audit Logs for the following behavioral indicators: (a) Device registrations from unexpected IP ranges, user agents associated with ROADtools (python-requests; validate 'roadtools' user-agent against your traffic), or accounts not normally performing device joins; (b) PRT issuance followed by token exchanges across multiple Microsoft services within short time windows; (c) Authentication events with device compliance claims from devices not in your MDM/Intune inventory; (d) Graph API calls for enumeration patterns (bulk user, group, or role queries), correlate with T1087. Enable Conditional Access sign-in logs and alert on tokens issued without compliant device claims. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) to ensure these log sources are collected and reviewed. Use MITRE D3FEND D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) principles to baseline normal device and token activity.
3. Step 3: Eradication, Once containment is stabilized, rotate credentials for any account with suspicious PRT issuance or token exchange activity (NIST IA controls; D3-CRO, Credential Rotation). Revoke all refresh tokens for affected accounts using the Microsoft Graph API (revokeSignInSessions) or the Entra ID portal. Remove unauthorized registered devices. Enforce Compliant Device Conditional Access policies so that only Intune-enrolled, policy-compliant devices can obtain PRTs. Apply NIST AC-7 (Unsuccessful Logon Attempts) and AC-17 (Remote Access) controls to restrict remote authentication paths. Enable Entra ID's 'Device-based Conditional Access' requiring Hybrid Azure AD Join or Intune compliance for all cloud app access.
4. Step 4: Recovery, Validate that no rogue devices remain in the tenant and that token issuance logs show no anomalous cross-service pivots. Confirm Conditional Access policies enforcing compliant device and MFA requirements are applied to all users, including privileged accounts (CIS 6.3, 6.4, 6.5, MFA requirements). Monitor Entra ID Sign-In Logs for 30 days post-remediation for recurrence of ROADtools user-agent strings or anomalous device registration events. Verify audit log retention meets policy (NIST AU-11, Audit Record Retention; CIS 8.2, Collect Audit Logs) to support forensic review if re-compromise is suspected.
5. Step 5: Hardening, Conduct a gap assessment against NIST AC-6 (Least Privilege) for device registration permissions and AC-2 (Account Management) for cloud account lifecycle controls. Implement Privileged Identity Management (PIM) for Entra ID roles that can register devices or modify authentication policies. Develop or update detection rules for ROADtools behavioral indicators in your SIEM. Map

detection gaps to MITRE ATT&CK T1550 (Use Alternate Authentication Material) and T1556 (Modify Authentication Process) to drive detection engineering backlog. Review D3-MFA (Multi-factor Authentication) and D3-CH (Credential Hardening) D3FEND countermeasures for additional hardening opportunities.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO, legal counsel, and executive leadership if any Global Administrator, Privileged Role Administrator, or Application Administrator account is confirmed to have had a PRT issued to a ROADtools-registered device, if tenant-wide Graph API enumeration is confirmed (indicating full directory exfiltration by APT29/APT33), or if the organization is subject to GDPR, HIPAA, or SEC cybersecurity incident disclosure rules and personal data or material nonpublic information was accessible via the compromised token scope.
Recovery Notes	After revoking all affected sessions and removing rogue devices, verify recovery completeness by confirming that Sign-In Logs show zero successful authentications with `isCompliant = false` or `UserAgent` matching ROADtools strings for a minimum of 72 hours post-eradication before declaring containment successful. Continue monitoring Entra ID Sign-In Logs and Identity Protection risk events daily for 30 days, specifically watching for 'Anomalous token' detections (which Microsoft uses to flag PRT abuse) and new device registrations outside approved workflows. Given APT29's documented practice of establishing multiple persistence mechanisms during a single intrusion — including OAuth app registrations and service principal credential additions — also audit Enterprise Applications and App Registrations for any credentials (client secrets or certificates) added during the suspected compromise window.
Forensic Artifacts	Entra ID Audit Logs — operation 'Register device': captures the initiating user, source IP, timestamp, and the alternativeSecurityIds field containing the software-generated public key that ROADtools uses to fabricate a device identity without hardware TPM attestation, directly distinguishing rogue devices from legitimate Intune-enrolled endpoints. | Entra ID Non-Interactive Sign-In Logs (AADNonInteractiveUserSignInLogs): records every PRT-derived silent token exchange across Microsoft services (SharePoint, Exchange Online, Azure Resource Manager, Teams Graph), revealing the full scope of lateral movement APT29/APT33 conducted after obtaining the initial PRT via the rogue device. | Microsoft Graph API audit trail in Entra ID Audit Logs filtered for 'List members', 'List users', 'List groups', and 'List roleAssignments': ROADtools' roadrecon module performs sequential bulk enumeration of the entire tenant directory — this produces a forensically distinct burst pattern of read operations within a compressed timeframe, attributable to T1087.004 (Account Discovery: Cloud Account). | Entra ID Identity Protection risk detections — specifically 'Anomalous token' and 'Unfamiliar sign-in properties' risk events: Microsoft's internal ML models flag PRT token anomalies including unusual token lifetime, unexpected resource access patterns, and sign-ins from IPs inconsistent with the user's history, providing a corroborating forensic timeline independent of raw log analysis. | Conditional Access policy evaluation logs (SigninLogs.conditionalAccessPolicies array): each sign-in record contains the evaluation result for every CA policy — a ROADtools-registered rogue device will show CA policies that require compliant device as 'notApplied' or 'failure' with `enforcedGrantControls` empty, forensically documenting exactly which policy gap enabled the MFA bypass that is the core mechanism of this campaign.

Per-Action IR Details

Step 1: Containment — Audit all registered devices in Entra ID immediately. In the Azure portal, navigate to Entra ID > Devices > All Devices and filter for recently registered devices (last 30–90 days). Disable or remove any device not recognized in your asset inventory (CIS 1.1 — Enterprise Asset Inventory, CIS 1.2 — Address Unauthorized Assets). Restrict device registration permissions to authorized users only via Entra ID device settings (Users may register their devices: set to 'Selected' or 'None' unless operationally required).

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST CM-7 (Least Functionality) — implied via device registration restriction, CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 1.2 (Address Unauthorized Assets)

Compensating: Export all registered devices via Microsoft Graph API using: `Invoke-RestMethod -Uri 'https://graph.microsoft.com/v1.0/devices?$select=displayName,registrationDateTime,operatingSystem,deviceOwnership,approximateLastSignInDateTime' -Headers @{Authorization="Bearer $token"}` or use the free Azure CLI command `az ad device list --output table`. Cross-reference output against your CMDB or a manually maintained spreadsheet. For tenants without Intune, use `Get-MgDevice` from the Microsoft.Graph PowerShell module (free) and flag any device where `managementType` is null or `isCompliant` is false.

Evidence: Before disabling any device, export and preserve: (1) Entra ID Audit Logs filtered for operation 'Register device' and 'Add registered owner to device' for the last 90 days — capture initiatedBy.user.userPrincipalName, targetResources[].deviceId, and sourceIPAddress; (2) The full device object from Graph API including deviceId, objectId, alternativeSecurityIds (contains the public key used in ROADtools registration), and approximateLastSignInDateTime; (3) Sign-In Logs correlated to each suspicious deviceId showing tokenIssuanceDetail and conditionalAccessStatus. ROADtools device registration produces a synthetic device with a software-generated TPM key — the alternativeSecurityIds field will lack a valid hardware TPM attestation, which is forensically distinguishable from legitimate Intune-enrolled devices.

Step 2: Detection — Enable and query Entra ID Sign-In Logs and Audit Logs for the following behavioral indicators: (a) Device registrations from unexpected IP ranges, user agents associated with ROADtools (python-requests, roadtools), or accounts not normally performing device joins; (b) PRT issuance followed by token exchanges across multiple Microsoft services within short time windows; (c) Authentication events with device compliance claims from devices not in your MDM/Intune inventory; (d) Graph API calls for enumeration patterns (bulk user, group, or role queries) — correlate with T1087. Enable Conditional Access sign-in logs and alert on tokens issued without compliant device claims. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) to ensure these log sources are collected and reviewed. Use MITRE D3FEND D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) principles to baseline normal device and token activity.

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), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring) — implied continuous monitoring requirement, CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use the Microsoft Entra ID free log export to a Log Analytics Workspace (90-day retention on Basic SKU, free tier available). Run the following KQL query against SigninLogs: `SigninLogs | where UserAgent contains 'python-requests' or UserAgent contains 'roadtools' or UserAgent contains 'roadtx' | project TimeGenerated, UserPrincipalName, IPAddress, UserAgent, DeviceDetail, ConditionalAccessStatus, ResultType`. For PRT chaining detection without SIEM, use the free Microsoft Sentinel detection rule 'Azure AD - MFA Bypassed Using Device Registration' or manually query `AADNonInteractiveUserSignInLogs` filtering on `AuthenticationRequirement == 'singleFactorAuthentication'` with `DeviceDetail.isCompliant == false`. Export results to CSV weekly using PowerShell `Export-AzureADSignInLog` equivalent via Graph API.

Evidence: Preserve the following before any remediation: (1) Entra ID Sign-In Logs (both interactive and non-interactive) for each suspicious account — specifically the `authenticationDetails`, `conditionalAccessPolicies`, and `deviceDetail.deviceId` fields, which will show PRT-derived tokens authenticating without satisfying Conditional Access device compliance checks; (2) Microsoft Graph API access logs from the Entra ID Audit Logs filtered for `activityDisplayName` containing 'List members', 'List users', or 'List groups' — APT29 and UTA0355 use ROADtools' `roadrecon` module to enumerate the full tenant, producing sequential bulk Graph API calls within minutes from the rogue device's token; (3) Azure AD Audit Logs for `Add service principal credentials` and `Update application` events, which may indicate token persistence beyond the initial PRT; (4) Conditional Access named locations log showing sign-ins from IPs not in any defined trusted location policy, cross-referenced against known APT29 infrastructure (refer to CISA AA23-347A for APT29 IOCs).

Step 3: Eradication — Rotate credentials for any account with suspicious PRT issuance or token exchange activity (NIST IA controls; D3-CRO — Credential Rotation). Revoke all refresh tokens for affected accounts using the Microsoft Graph API (revokeSignInSessions) or the Entra ID portal. Remove unauthorized registered devices. Enforce Compliant Device Conditional Access policies so that only Intune-enrolled, policy-compliant devices can obtain PRTs. Apply NIST AC-7 (Unsuccessful Logon Attempts) and AC-17 (Remote Access) controls to restrict remote authentication paths. Enable Entra ID's 'Device-based Conditional Access' requiring Hybrid Azure AD Join or Intune compliance for all cloud app access.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management) — credential rotation for compromised accounts, NIST IA-11 (Re-authentication) — force re-authentication after token revocation, CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Revoke all active sessions and refresh tokens for affected accounts using the free Microsoft Graph PowerShell module: `Revoke-MgUserSignInSession -UserId ` — run this for every account that touched a suspicious rogue device. For bulk revocation: `Get-Content affected_users.txt | ForEach-Object { Revoke-MgUserSignInSession -UserId $_ }`. Delete rogue devices with: `Remove-MgDevice -DeviceId `. To enforce compliant-device CA without Intune licensing, create a Conditional Access policy (free in all Entra ID P1 tenants) requiring 'Hybrid Azure AD Joined' device as a grant control for all cloud apps — this blocks ROADtools-registered software devices from obtaining new PRTs post-eradication. Verify PRT revocation was effective by querying Sign-In Logs for the affected user 30 minutes post-revocation and confirming `authenticationRequirement` no longer shows device-based single-factor claims.

Evidence: Before revoking tokens and removing devices, preserve: (1) The full token signing key and alternativeSecurityId from each rogue device object via `Get-MgDevice -DeviceId -Property *` — this documents the software-generated key material ROADtools used to fabricate the device identity; (2) A snapshot of `AADNonInteractiveUserSignInLogs` showing all resource IDs accessed via PRT-derived tokens (the `resourceDisplayName` field will enumerate every Microsoft service the actor pivoted to — SharePoint, Exchange Online, Teams, Azure Resource Manager — consistent with APT33's and APT29's documented lateral movement to M365 data stores); (3) Entra ID Audit Logs for `Delete device` operations performed during eradication, timestamped, to establish the remediation chain of custody under NIST 800-61r3 §3.4 documentation requirements.

Step 4: Recovery — Validate that no rogue devices remain in the tenant and that token issuance logs show no anomalous cross-service pivots. Confirm Conditional Access policies enforcing compliant device and MFA requirements are applied to all users, including privileged accounts (CIS 6.3, 6.4, 6.5 — MFA requirements). Monitor Entra ID Sign-In Logs for 30 days post-remediation for recurrence of ROADtools user-agent strings or anomalous device registration events. Verify audit log retention meets policy (NIST AU-11 — Audit Record Retention; CIS 8.2 — Collect Audit Logs) to support forensic review if re-compromise is suspected.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), NIST CA-7 (Continuous Monitoring) — verify restored secure state, 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), CIS 8.2 (Collect Audit Logs)

Compensating: Validate device cleanliness by running `Get-MgDevice -Filter "registrationDateTime ge $(Get-Date).AddDays(-30)" | Select-Object displayName, registrationDateTime, isCompliant, managementType` and confirming zero results for non-compliant or unmanaged devices registered post-eradication. For continuous 30-day monitoring without a SIEM, create a Logic App (free consumption tier) that runs daily, queries Sign-In Logs for `UserAgent contains 'python-requests' OR UserAgent contains 'roadtools'`, and emails results to the SOC. Additionally, configure Entra ID's built-in 'New device registered' diagnostic alert under Identity Protection (free tier) to notify on any new device registration event outside business hours or from non-corporate IP ranges.

Evidence: During recovery validation, collect: (1) A Conditional Access policy evaluation report (exported from Entra ID > Monitoring > Sign-in logs, filtering on `conditionalAccessStatus = failure`) confirming that post-remediation sign-in attempts from non-compliant devices are now blocked rather than allowed with MFA bypass; (2) A clean baseline export of all registered devices post-eradication (timestamped) to serve as the new authorized device inventory baseline per CIS 1.1; (3) Entra ID Identity Protection risk event logs showing whether any of the affected accounts triggered 'Unfamiliar sign-in properties' or 'Anomalous token' risk detections during the active campaign — these retroactive risk scores confirm the attack timeline for post-incident reporting and potential breach notification assessment.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-6 (Least Privilege) for device registration permissions and AC-2 (Account Management) for cloud account lifecycle controls. Implement Privileged Identity Management (PIM) for Entra ID roles that can register devices or modify authentication policies. Develop or update detection rules for ROADtools behavioral indicators in your SIEM. Map detection gaps to MITRE ATT&CK T1550 (Use Alternate Authentication Material) and T1556 (Modify Authentication Process) to drive detection engineering backlog. Review D3-MFA (Multi-factor Authentication) and D3-CH (Credential Hardening) D3FEND countermeasures for additional hardening opportunities.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST RA-3 (Risk Assessment) — reassess residual risk after incident, CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without commercial SIEM, publish the following free Sigma detection rules to your log analysis pipeline: search the SigmaHQ repository for rules tagged with 'azure' and 'device_registration' targeting `UserAgent|contains|roadtools` — or author a custom rule targeting Entra ID SigninLogs with condition `UserAgent contains 'python-requests' AND DeviceDetail.isCompliant = false AND AuthenticationRequirement = 'singleFactorAuthentication'`. For PIM without Entra ID P2 licensing, implement a manual JIT process: create a security group for 'Device Registration Approvers', remove all users from the default device registration permission, and require a ticket-based approval workflow (documented in your ITSM) before temporarily adding a user to that group. Document the ROADtools TTPs — device registration via `roadtx`, PRT acquisition via `roadtx prt`, and tenant enumeration via `roadrecon` — in your threat library mapped to ATT&CK T1550.001 (Use Alternate Authentication Material: Application Access Token) and T1556.006 (Modify Authentication Process: Multi-Factor Authentication).

Evidence: For the post-incident lessons learned report (NIST 800-61r3 §4), compile: (1) The complete timeline of rogue device registrations correlated to user account activity, sourced from Entra ID Audit Logs, establishing initial access timing relative to any known APT29/APT33 campaign activity reported in CISA or Microsoft MSRC advisories; (2) A comparison of Conditional Access policy state before and after the incident, documenting which specific CA policy gaps (missing compliant device requirement, missing MFA for legacy auth, etc.) permitted the ROADtools PRT to authenticate without triggering a block; (3) Identity Protection risk detection history for all affected accounts, showing whether Entra ID's built-in anomaly detection flagged the attack and was suppressed, missed, or not actioned — this directly informs the detection engineering backlog for T1550 and T1556 coverage gaps.

Detection Guidance

Signature-based detection is not effective for this campaign. All malicious activity uses legitimate Microsoft API calls. Focus detection on behavioral anomalies across three log sources:

1. Entra ID Audit Logs, Query for device registration events (category: Device, activity: Register device) from accounts that do not routinely perform device joins, from unusual geographic locations, or with python-requests or potential roadtools-associated User-Agent strings in associated sign-in records. Validate tool-specific user-agents against your traffic before alerting.

2. Entra ID Sign-In Logs, Alert on: (a) PRT-based token issuance (tokenIssuanceType: PrimaryRefreshToken) for devices not present in Intune/MDM inventory; (b) Rapid cross-service token exchanges following device registration (Graph API, Exchange Online, SharePoint within the same session); (c) Sign-ins from registered devices with no corresponding MDM compliance record.

3. Microsoft Graph API Activity Logs, Via Entra Diagnostic Settings or Azure Monitor configuration, flag bulk enumeration patterns: high-volume calls to /users, /groups, /directoryRoles, or /devices endpoints from a single principal in a short window (correlates with T1087, Account Discovery). Note: Graph API caller logging requires Azure Monitor or Purview configuration; verify availability in your tenant before implementing this detection layer.

Behavioral indicators: accounts registering multiple devices in a single session; device registrations immediately preceding privileged role queries; authentication flows where MFA is satisfied via PRT but the originating device is not in the corporate asset inventory (CIS 1.1).

D3FEND countermeasures: D3-LAM (Local Account Monitoring), D3-UAP (User Account Permissions review), D3-SFA (System File Analysis for authentication configuration changes). NIST AU-6 (Audit Record Review) and AU-12 (Audit Record Generation) provide the control framework for ensuring these log sources are active and reviewed on a defined frequency.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`python-requests (User-Agent string pattern in Entra Sign-In Logs)`	ROADtools default HTTP client User-Agent string; presence in Entra ID Sign-In Logs associated with device registration or Graph API enumeration activity is a behavioral indicator of ROADtools usage	MEDIUM
URL	`roadtools (User-Agent string pattern in Entra Sign-In Logs)`	ROADtools explicit User-Agent string variant; flag any authentication or API call presenting this string in Entra diagnostic logs	HIGH

Framework Mappings

MITRE-ATTACK

- **T1528** — Steal Application Access Token
- **T1556.006** — Multi-Factor Authentication
- **T1087** — Account Discovery

- **T1556** — Modify Authentication Process
- **T1566.001** — Spearphishing Attachment
- **T1078** — Valid Accounts
- **T1550.001** — Application Access Token
- **T1621** — Multi-Factor Authentication Request Generation
- **T1550** — Use Alternate Authentication Material
- **T1078.004** — Cloud Accounts
- **T1110.003** — Password Spraying
- **T1098** — Account Manipulation
- **T1098.005** — Device Registration

NIST-800-53R5

- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management

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
T1528	Steal Application Access Token	Credential-Access
T1556.006	Multi-Factor Authentication	Credential-Access
T1087	Account Discovery	Discovery
T1556	Modify Authentication Process	Credential-Access
T1566.001	Spearphishing Attachment	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1550	Use Alternate Authentication Material	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion
T1110.003	Password Spraying	Credential-Access
T1098	Account Manipulation	Persistence
T1098.005	Device Registration	Persistence

Sources

Source	URL	Tier
Unit 42	https://unit42.paloaltonetworks.com/roadtools-cloud-attacks/	T3
	https://unit42.paloaltonetworks.com/roadtools-cloud-attacks/	T3
	https://unit42.paloaltonetworks.com/malware-used-by-rocke-group-evo...	T3
Microsoft Entra releases and announcements	https://learn.microsoft.com/en-us/entra/fundamentals/whats-new	T1

Source	URL	Tier
This Microsoft Entra ID Vulnerability Could Have Been Catastrophic	https://www.reddit.com/r/sysadmin/comments/1nlbl8r/this_microsoft_e...	T3

Generated 2026-05-23 06:27 UTC by TJS Security Command Center