INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 06:38 UTC

Q1 2026 IR Trends: Phishing Returns to the Top, AI-Assisted Credential Harvesting Arrives, and Cloud Living-Off-the-Land Expands Attack Surface

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0075
Type	Security Analysis
CVE ID	CVE-2025-20393, CVE-2023-20198
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Exchange, Outlook Web Access (OWA), Microsoft Azure, Microsoft Graph API, GitHub (Personal Access Tokens), Cisco Secure Email Gateway, Cisco Secure Email and Web Manager (AsyncOS), Cisco IOS XE
Published	2026-04-22T10:00:34+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Cisco Talos incident response data from Q1 2026 identifies three converging shifts in attacker tradecraft: phishing reclaimed the top initial access position after a period of exploitation-led intrusions, no-code platforms are lowering the technical barrier for credential harvesting operations, and a newly documented extortion group achieved full cloud environment compromise using only a single exposed token and native cloud services. Together, these trends signal that attackers are optimizing for speed and stealth over sophistication, reducing their footprint while expanding their reach into cloud infrastructure. Organizations that have prioritized perimeter-based detection and malware-centric response models face measurable blind spots against this evolving pattern.

Technical Analysis

Cisco Talos IR Q1 2026 data presents three distinct but reinforcing trends that security teams should analyze together rather than in isolation.

Phishing as the leading initial access vector: Talos observed phishing accounting for over one-third of engagements where initial access was determined, reversing a prior trend toward exploitation-led intrusions.

This is not a regression to simpler tactics, it reflects attacker awareness that hardened perimeters and faster patching cycles have raised the cost of reliable exploit chains. Phishing, by contrast, exploits the human layer, which remains comparatively unpatched. The affected platforms include Microsoft Exchange and Outlook Web Access, consistent with MITRE T1566 and T1566.002 (spearphishing link). Cisco Secure Email Gateway and Cisco Secure Email and Web Manager (AsyncOS) also appear in the affected product set, with CVE-2025-20393 (Cisco AsyncOS, CVSS critical) and CVE-2023-20198 (Cisco IOS XE, CVSS 10.0) referenced, likely as supporting initial access or persistence vectors against organizations with vulnerable Cisco email infrastructure. CVE-2023-20198 has historical exploit-in-the-wild documentation; its appearance in this dataset may indicate continued opportunistic exploitation of unpatched infrastructure.

No-code credential harvesting via Softr: According to Talos Q1 2026 IR data, Softr, a legitimate no-code application builder, was documented being used by a threat actor to construct credential harvesting pages targeting Microsoft Exchange and OWA (source pending independent verification). This represents a qualitative shift: threat actors are offloading the technical work of building phishing infrastructure to commercial SaaS platforms, reducing entry cost and complicating detection. Pages built on Softr inherit legitimacy signals, SSL certificates, reputable hosting infrastructure, and recognizable domain patterns, that degrade the effectiveness of URL-reputation-based filtering. This maps to MITRE T1566 (phishing), T1528 (steal application access token), T1557 (adversary-in-the-middle), and CWE-287 (improper authentication). The defensive gap this exploits is the assumption that phishing infrastructure will exhibit known-bad infrastructure signals. It often will not.

Crimson Collective cloud-native extortion chain: The most operationally significant finding is the Crimson Collective campaign, which demonstrated a cloud-native attack chain beginning with a single exposed GitHub Personal Access Token. From that single credential, the actor pivoted through the Microsoft Graph API and native Azure services to achieve full cloud environment compromise, without deploying traditional malware at any stage. This maps directly to MITRE T1552.001 (credentials in files), T1528 (steal application access token), T1021.007 (cloud services lateral movement), T1648 (serverless execution), T1530 (data from cloud storage object), and T1619 (cloud storage object discovery). The absence of malware is not incidental - it is the technique. Living-off-the-land in cloud environments (cloud LotL) means EDR and AV coverage is irrelevant; the attacker's actions are indistinguishable from legitimate API calls unless behavioral baselines exist for cloud identity activity. CWE-522 (insufficiently protected credentials) and CWE-693 (protection mechanism failure) are foundational to why this chain succeeds. The GitHub PAT exposure aligns with T1195 (supply chain compromise) and T1588.002 (tool acquisition), suggesting the token may have been sourced from a repository or CI/CD environment rather than through direct credential theft. Affected systems include GitHub (Personal Access Tokens), Microsoft Graph API, and Microsoft Azure native services. Note: Crimson Collective attribution and campaign details are sourced from the Talos Q1 2026 report, which has not been independently verified. Validate directly against Talos publication before operational use.

The convergence is the story: phishing delivers initial access at scale, no-code platforms commoditize the infrastructure, and cloud-native post-exploitation chains eliminate the forensic artifacts that traditional IR depends on. Organizations relying on malware detection, known-bad IOC matching, or endpoint telemetry as primary detection layers have structural blind spots against all three of these trends simultaneously.

Action Checklist

1. Step 1: Assess exposure. Audit your Microsoft Exchange, OWA, Azure, and GitHub environments for the specific conditions described: internet-facing OWA, exposed GitHub Personal Access Tokens in repositories or CI/CD pipelines, and Cisco Secure Email Gateway or IOS XE deployments running

AsyncOS versions affected by CVE-2025-20393 or IOS XE versions affected by CVE-2023-20198 (specific version information available at CVE-2025-20393 and CVE-2023-20198 detail pages; consult NVD or Cisco PSIRT for affected version ranges and patch availability)

2. Step 2: Review controls. Verify MFA enforcement across all Exchange and OWA authentication paths; audit Microsoft Graph API permissions and OAuth application grants for least-privilege compliance; review GitHub PAT policies (expiration, scope limits, secret scanning enablement); and confirm Cisco Secure Email Gateway patches are current for CVE-2025-20393

3. Step 3: Update threat model. Add Crimson Collective's cloud-native token-pivot chain as a named scenario in your threat register; add no-code phishing infrastructure (specifically Softr-hosted pages) as a detection gap in your phishing response playbook; map T1021.007, T1648, T1530, and T1528 against your current cloud detection coverage

4. Step 4: Communicate findings. Brief leadership with three specific risk statements: (1) a single exposed GitHub token can now yield full Azure environment compromise without malware, (2) phishing pages are increasingly hosted on legitimate SaaS platforms that bypass URL reputation filters, and (3) cloud-native attack chains leave no endpoint artifacts for traditional IR to recover

5. Step 5: Monitor developments. Track Cisco Talos quarterly IR reports for follow-on Q2 2026 data; monitor Microsoft Entra ID and Azure audit logs for anomalous Graph API calls; watch for Softr platform abuse disclosures; and track any law enforcement or industry reporting on Crimson Collective attribution and infrastructure

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if Entra ID logs show any OAuth consent grant or Graph API token issuance to an unrecognized service principal within the prior 90 days, if any GitHub PAT with repo-admin or Azure-linked scope is found exposed in a repository or CI/CD pipeline, or if Cisco IOS XE devices running versions affected by CVE-2023-20198 (an actively KEV-listed vulnerability with known mass exploitation history) are confirmed internet-facing without patch or ACL mitigation — any of these conditions constitutes a probable breach scenario with potential PII/data exfiltration exposure triggering regulatory notification assessment.
Recovery Notes	Post-containment, rotate all GitHub Personal Access Tokens organization-wide and re-issue with minimum required scopes and 90-day expiration, then re-audit all Azure OAuth application grants and revoke any service principal tokens issued during the suspect window identified in Entra ID logs. Monitor Azure activity logs and Graph API audit logs continuously for at least 30 days post-recovery for re-emergence of T1021.007 or T1648 patterns, as Crimson Collective-style operators are known to establish secondary persistence via additional OAuth app registrations before primary token revocation. Verify Cisco Secure Email Gateway and IOS XE patching is confirmed on all nodes via 'show version' output archived to change management, and re-run the truffleHog PAT scan and Entra ID OAuth grant audit at 7-day and 30-day post-recovery checkpoints to confirm clean state.

Forensic Artifacts	Microsoft Entra ID Non-Interactive Sign-In Logs (ServicePrincipalSignIns table in Log Analytics) — Crimson Collective's cloud-native token-pivot chain uses service principal authentication to call Graph API and ARM endpoints, which appears only in non-interactive logs, not the standard sign-in blade; filter for service principals created within 30 days of the anomaly window and cross-reference against the OAuth consent grant timestamps | GitHub Audit Log entries for 'personal_access_token.access' and 'git.clone' events — a PAT-based Azure pivot chain begins with repository cloning or secrets enumeration; the audit log will record the source IP and timestamp of each PAT usage, providing the initial access timestamp and origin IP for the Crimson Collective kill chain reconstruction | Azure ARM Activity Log filtered for 'microsoft.resources/subscriptions/resources/read' and 'microsoft.authorization/roleassignments/write' operations — these are the exact API calls made during the cloud enumeration and privilege escalation phases (T1021.007, T1648) of a token-pivot attack; the caller identity in these log entries will be the service principal or managed identity abused post-PAT-compromise | Cisco Secure Email Gateway AsyncOS web framework logs at /data/log/gui_logs/gui.log — CVE-2025-20393 is an authentication bypass in the AsyncOS web management interface; post-exploitation commands executed via the bypass will appear as authenticated HTTP POST requests from attacker IPs to the management UI endpoints before any valid session cookie was issued, which is the forensic signature distinguishing exploit traffic from legitimate admin sessions | Microsoft Exchange/OWA IIS logs (typically at C:\inetpub\logs\LogFiles\W3SVC1\ on Exchange servers) filtered for POST requests to /owa/auth/ and /EWS/Exchange.asmx from external IPs — AI-assisted credential harvesting campaigns targeting OWA will produce high-volume authentication attempts (Event ID 4625 in Windows Security log for failed auths) followed by a single successful Event ID 4624 (Type 8, NetworkCleartext, indicating Basic Auth) from the same source IP, which is the forensic pattern distinguishing harvested-credential use from brute force

Per-Action IR Details

Step 1: Assess exposure — audit your Microsoft Exchange, OWA, Azure, and GitHub environments for the specific conditions described: internet-facing OWA, exposed GitHub Personal Access Tokens in repositories or CI/CD pipelines, and Cisco Secure Email Gateway or IOS XE deployments running AsyncOS versions affected by CVE-2025-20393 or IOS XE versions affected by CVE-2023-20198

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing IR capability and identifying assets before an incident occurs

Controls: NIST SI-2 (Flaw Remediation), NIST RA-3 (Risk Assessment), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For OWA exposure: run 'Invoke-WebRequest -Uri https:///owa/auth/logon.aspx -UseBasicParsing' from an external IP to confirm internet reachability. For GitHub PAT exposure: use the open-source tool 'truffleHog' (pip install trufflehog) with 'trufflehog git https://github.com//' to scan repositories for exposed tokens matching GitHub PAT patterns. For Cisco AsyncOS version enumeration: SSH to the gateway and run 'version' at the CLI prompt; compare output against Cisco advisory cisco-sa-sma-esa-auth-bypass-bv2TnGNR for CVE-2025-20393 and against CISA KEV entry for CVE-2023-20198 on IOS XE. For Azure: run 'az ad app list --query "[].{AppId:appId, DisplayName:displayName}" -o table' to enumerate all OAuth app registrations without a CSPM tool.

Evidence: Before any changes, capture point-in-time state: (1) GitHub audit log export via 'gh api /orgs//audit-log --paginate > github_audit_baseline.json' to establish PAT creation and usage history; (2) Microsoft Entra ID sign-in logs filtered to OWA and Exchange Online service principals — export from Entra portal or via 'Get-MgAuditLogSignIn -Filter "appDisplayName eq \'Outlook Web App\'" ' for the prior 90 days; (3) Cisco Secure Email Gateway 'mail_logs' and 'tracking_logs' from /data/log/ for the prior 30 days to baseline normal message flow before patch; (4) IOS XE

running-config snapshot via 'show running-config' and 'show version' outputs archived to a change-controlled store to document pre-patch state.

Step 2: Review controls — verify MFA enforcement across all Exchange and OWA authentication paths; audit Microsoft Graph API permissions and OAuth application grants for least-privilege compliance; review GitHub PAT policies (expiration, scope limits, secret scanning enablement); and confirm Cisco Secure Email Gateway patches are current for CVE-2025-20393

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring preventive controls are in place to reduce incident likelihood and impact

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: MFA audit without Entra P2 license: run 'Get-MgUser -All | Get-MgUserAuthenticationMethod' and pipe to CSV to identify accounts with only password authentication on OWA-accessible mailboxes. Graph API permission audit: execute 'Get-MgServicePrincipal -All | ForEach-Object { Get-MgServicePrincipalAppRoleAssignment -ServicePrincipalId $_.Id }' and flag any app with Mail.ReadWrite, Files.ReadWrite.All, or User.ReadWrite.All delegated permissions — these are the exact scopes Crimson Collective-style operators abuse for mailbox access and OneDrive exfiltration. GitHub PAT audit without GitHub Advanced Security license: enable the free 'Secret scanning alerts' under Settings > Security > Code security and analysis in each repo; additionally run 'gh api /orgs//secret-scanning/alerts --paginate' to pull existing findings. Cisco CVE-2025-20393 patch verification: SSH to Secure Email Gateway and run 'version; show asyncos version' — compare against Cisco advisory's fixed release table and confirm running version is 15.5.1-055 or later (or per the advisory's fixed release for your train).

Evidence: Capture before enforcing MFA or revoking tokens: (1) Microsoft Entra ID Conditional Access policy export via 'Get-MgIdentityConditionalAccessPolicy -All | ConvertTo-Json -Depth 10' to document pre-change policy state and identify gaps where OWA or legacy authentication (Basic Auth) is not blocked; (2) full OAuth application consent grant list from 'Get-MgOauth2PermissionGrant -All | Select-Object ClientId, Scope, PrincipalId' — this documents which apps had Graph API access before any remediation, preserving evidence of potentially malicious app registrations consistent with T1528 (Steal Application Access Token); (3) GitHub audit log entries for PAT creation events — filter for 'personal_access_token.create' and 'personal_access_token.access' action types in the prior 90-day export captured in Step 1.

Step 3: Update threat model — add Crimson Collective's cloud-native token-pivot chain as a named scenario in your threat register; add no-code phishing infrastructure (specifically Softr-hosted pages) as a detection gap in your phishing response playbook; map T1021.007, T1648, T1530, and T1528 against your current cloud detection coverage

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: updating IR plans and detection capability based on emerging threat intelligence

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-4 (System Monitoring), NIST PM-16 (Threat Awareness Program), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 8.2 (Collect Audit Logs)

Compensating: ATT&CK coverage gap analysis without a commercial SIEM: download the free ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/) and create a layer marking T1021.007 (Remote Services: Cloud Services), T1648 (Serverless Execution), T1530 (Data from Cloud Storage), and T1528 (Steal Application Access Token) — score each red/yellow/green based on whether you have a log source and alert for it. For Softr-based phishing detection gap: create a Sigma rule targeting proxy/DNS logs for requests to '*.softr.app' or '*.softr.io' domains originating from corporate users — the free Sigma rule converter (sigmac or pySigma) can translate this to your log format. For the Crimson Collective token-pivot scenario: document the kill chain as: exposed GitHub PAT → Azure ARM API enumeration ('az resource list') → Graph API OAuth token request → mailbox/OneDrive access → cloud

storage exfiltration, and verify you have a log source for each hop.

Evidence: Before updating the threat model, collect current detection baseline evidence: (1) Azure Monitor activity log query for Graph API calls — run 'az monitor activity-log list --offset 30d --query "[?operationName.value==\'microsoft.graph/users/read\' || operationName.value==\'microsoft.graph/me/messages/read\']"' to establish whether T1648/T1530 activity is already present but undetected; (2) DNS query logs or proxy logs for the prior 30 days queried for '.softr.app' or '.softr.io' to determine if Softr-hosted phishing has already targeted your users; (3) Entra ID audit log filtered for 'Add service principal' and 'Consent to application' events in the prior 90 days to detect T1528 precursor activity — export via 'Get-MgAuditLogDirectoryAudit -Filter "activityDisplayName eq \'Consent to application\'\"".

Step 4: Communicate findings — brief leadership with three specific risk statements: (1) a single exposed GitHub token can now yield full Azure environment compromise without malware, (2) phishing pages are increasingly hosted on legitimate SaaS platforms that bypass URL reputation filters, and (3) cloud-native attack chains leave no endpoint artifacts for traditional IR to recover

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring leadership is informed of IR capability gaps and risk posture before an incident occurs

Controls: NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST PM-9 (Risk Management Strategy), NIST CA-7 (Continuous Monitoring), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For a 2-person team preparing a leadership brief without a GRC platform: structure the brief around three quantified blast-radius statements derived from your Step 1 and Step 2 audit outputs — (1) count of GitHub PATs with 'repo' or 'admin:org' scope found in Step 1 multiplied by the number of Azure subscriptions they can reach; (2) count of users not enrolled in MFA on OWA-accessible paths from Step 2; (3) count of OAuth apps with Mail.ReadWrite or equivalent Graph API permissions lacking conditional access policy coverage. Attach the ATT&CK Navigator gap layer from Step 3 as a visual aid. Template the brief in one page using the BLUF (Bottom Line Up Front) format: risk statement, evidence, recommended decision, cost of inaction.

Evidence: The evidence for this communication step is the compiled output from Steps 1–3: GitHub PAT audit results, Entra ID MFA coverage gaps, OAuth permission grant list, and ATT&CK coverage gap layer. Additionally, preserve the Cisco Talos Q1 2026 IR report as a cited external source to anchor the risk statements — leadership briefs must reference authoritative sourcing, not internal assertion alone. Document the date and participants of the briefing per NIST IR-6 (Incident Reporting) requirements to establish an audit trail of risk acceptance or escalation decisions.

Step 5: Monitor developments — track Cisco Talos quarterly IR reports for follow-on Q2 2026 data; monitor Microsoft Entra ID and Azure audit logs for anomalous Graph API calls; watch for Softr platform abuse disclosures; and track any law enforcement or industry reporting on Crimson Collective attribution and infrastructure

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: continuous monitoring and threat intelligence integration to detect adversary activity

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), NIST PM-16 (Threat Awareness Program), CIS 8.2 (Collect Audit Logs)

Compensating: Graph API anomaly detection without a SIEM: create an Azure Monitor alert rule targeting the Entra ID sign-in log — use the KQL query 'AuditLogs | where OperationName == "Add OAuth2PermissionGrant" or OperationName == "Consent to application" | where TimeGenerated > ago(1d)' in a Log Analytics workspace (free 5GB/month tier) and configure email alerting. For Crimson Collective-style token pivot detection: enable Azure Defender for Resource Manager (or use the free 'az monitor activity-log alert create' CLI command) and alert on 'microsoft.resources/subscriptions/resources/read' operations from service principals created within the last 30 days — this catches the ARM enumeration phase of the token-pivot chain (T1021.007). For Softr abuse monitoring: subscribe to the free abuse.ch URLhaus feed and filter for entries tagged 'phishing' with hosting on Cloudflare or Akamai CDN ranges (which Softr uses), or configure a free DNS sinkhole using Pi-hole with a blocklist that includes known Softr

abuse subdomains as they are reported. For Cisco Talos and Crimson Collective tracking: configure a free RSS feed aggregator (FreshRSS, self-hosted) for https://blog.talosintelligence.com/rss and CISA's Known Exploited Vulnerabilities JSON feed at https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json for CVE-2025-20393 and CVE-2023-20198 status changes.

Evidence: Establish and preserve the following ongoing evidence streams before a confirmed incident: (1) Azure Entra ID audit logs configured for 90-day retention (the maximum for free tier) — specifically the 'ServicePrincipalSignIns' and 'ManagedIdentitySignIns' tables in Log Analytics, which capture the non-interactive authentication patterns used in Crimson Collective-style cloud-native attacks and would not appear in standard interactive sign-in logs; (2) GitHub audit log streaming enabled to an S3 bucket or Azure Blob via GitHub's audit log streaming feature — specifically retain events of type 'personal_access_token.access', 'org.add_member', and 'repo.create' which map to T1528 and T1136 (Create Account) activity; (3) Cisco Secure Email Gateway 'antispam_logs' and 'error_logs' from /data/log/gui_logs/ which would capture authentication bypass attempts against CVE-2025-20393's affected web UI component and post-exploitation command execution artifacts in the AsyncOS web framework logs.

Detection Guidance

Cloud identity and API behavioral hunting should be the first priority given the Crimson Collective cloud-LotL chain. Query Microsoft Entra ID sign-in logs and Azure Monitor for Graph API calls originating from service principals or PATs that deviate from established baselines, specifically: unusual call volumes to directory enumeration endpoints (T1087), first-time or rare API scopes being invoked, and Graph API activity originating from unexpected source IPs or geographic locations. For GitHub, enable secret scanning and audit PAT usage logs for tokens accessing repositories outside their expected scope or time window (T1552.001, T1528).

For phishing detection tuned to no-code infrastructure: standard URL reputation feeds will likely miss Softr-hosted pages. Shift detection toward credential submission behavior, specifically, inspect proxy and DNS logs for POST requests to Softr app domains (*.softr.app or custom domains fronted by Softr infrastructure) from corporate endpoints. Email gateway logs should be reviewed for links to no-code platform domains regardless of reputation score. T1566 and T1566.002 detections should include allowlisted-domain-hosted phishing as an explicit scenario.

For Cisco infrastructure: query for exploitation indicators consistent with CVE-2025-20393 (Cisco AsyncOS) and CVE-2023-20198 (Cisco IOS XE), including unexpected admin account creation (T1078), web shell artifacts on IOS XE devices (T1505.003), and email gateway configuration changes not initiated through change management workflows. CVE-2023-20198 exploitation has historically been followed rapidly by implant deployment; any IOS XE device that was internet-exposed during the prior exploitation window should be treated as potentially compromised until verified.

Log sources to prioritize: Microsoft Entra ID audit and sign-in logs, Azure Monitor activity logs, GitHub audit log (organization level), Microsoft Defender for Cloud Apps anomaly alerts, Cisco Secure Email Gateway MTA logs, IOS XE syslog for web UI authentication events, and proxy/DNS logs for submission events to SaaS-hosted domains.

CWE-778 (insufficient logging) is in the associated weakness set for a reason: organizations that have not enabled verbose cloud API logging will have no forensic record of a cloud-LotL intrusion. Verify logging is enabled and retained before a hunt begins.

Indicators of Compromise

Type	Value	Context	Confidence
TOOL	`Softr no-code platform`	Softr leveraged via threat actor-controlled account to construct credential harvesting pages impersonating Microsoft Exchange and OWA login portals, hosted on legitimate Softr infrastructure to evade URL reputation filtering	MEDIUM
TOOL	`Microsoft Graph API`	Graph API leveraged via stolen GitHub Personal Access Token to enumerate cloud environment and pivot through Azure native services as part of Crimson Collective cloud-native attack chain — no malware deployed	MEDIUM
TOOL	`GitHub Personal Access Token (PAT)`	Exposed PAT used as initial pivot point by Crimson Collective to authenticate to Microsoft Graph API and initiate lateral movement through Azure cloud environment	MEDIUM
URL	`Pending — refer to Cisco Talos Blog (https://blog.talosintelligence.com/ir-trends-q1-2026/) for published indicators`	Specific IOC values (C2 domains, phishing URLs, PAT patterns, Azure API indicators) referenced in Talos Q1 2026 IR report; URL requires active validation before use	LOW

Framework Mappings

MITRE-ATTACK

- **T1556** — Modify Authentication Process
- **T1087** — Account Discovery
- **T1505.003** — Web Shell
- **T1552.001** — Credentials In Files
- **T1059** — Command and Scripting Interpreter
- **T1528** — Steal Application Access Token
- **T1071.001** — Web Protocols
- **T1557** — Adversary-in-the-Middle
- **T1539** — Steal Web Session Cookie
- **T1566.002** — Spearphishing Link
- **T1195** — Supply Chain Compromise
- **T1021.007** — Cloud Services
- **T1648** — Serverless Execution
- **T1566** — Phishing
- **T1110** — Brute Force

- **T1619** — Cloud Storage Object Discovery
- **T1550.001** — Application Access Token
- **T1190** — Exploit Public-Facing Application
- **T1021.001** — Remote Desktop Protocol
- **T1588.002** — Tool
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

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
- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **CA-7** — Continuous Monitoring
- **AC-7** — Unsuccessful Logon Attempts
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-2** — Account Management
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IA-8** — Identification and Authentication (Non-Organizational Users)

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)(5)(i)** — Security Awareness and Training

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **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
T1556	Modify Authentication Process	Credential-Access
T1087	Account Discovery	Discovery
T1505.003	Web Shell	Persistence
T1552.001	Credentials In Files	Credential-Access
T1059	Command and Scripting Interpreter	Execution
T1528	Steal Application Access Token	Credential-Access
T1071.001	Web Protocols	Command-And-Control
T1557	Adversary-in-the-Middle	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1566.002	Spearphishing Link	Initial-Access
T1195	Supply Chain Compromise	Initial-Access
T1021.007	Cloud Services	Lateral-Movement

Technique ID	Technique Name	Tactic
T1648	Serverless Execution	Execution
T1566	Phishing	Initial-Access
T1110	Brute Force	Credential-Access
T1619	Cloud Storage Object Discovery	Discovery
T1550.001	Application Access Token	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1588.002	Tool	Resource-Development
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Cisco Talos Blog	https://blog.talosintelligence.com/ir-trends-q1-2026/	T3
	https://blog.talosintelligence.com/ir-trends-q1-2026/	T3
	https://blog.talosintelligence.com/quarterly-report-incident-respon...	T3
Vulnerability Details : CVE-2025-20393 - Asyncos	https://www.cvedetails.com/cve/CVE-2025-20393/	T3
CVE-2025-20393 Exploitation: A Maximum-Severity Zero-Day ...	https://socprime.com/blog/cve-2025-20393-vulnerability-exploitation/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-20393, CVE-2023-20198	T1
Microsoft Security Advisory	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-2039...	T1

Generated 2026-04-23 06:38 UTC by TJS Security Command Center