CONVERGE
TECHNOLOGY SOLUTIONS

THREAT INTEL REPORT 2025

Prepared by: Converge Cybersecurity Practice
convergetp.com/cybersecurity | 800.747.8585

JUNE

Observations for June 2025

Recent threat activity shows that attackers are increasingly exploiting the parts of enterprise infrastructure that receive the least attention—non-human identities, abandoned cloud assets, and embedded third-party integrations. **Machine identities such as service accounts, API keys, and OAuth tokens are being used to move laterally and access sensitive systems without detection.** These credentials are often over-permissioned, lack expiration, and exist outside the scope of traditional identity management. As automation and integration grow, so does the scale and risk of these unmanaged access points.

At the infrastructure level, the **Hazy Hawk threat group continues to target misconfigured DNS records and expired cloud services to hijack subdomains** tied to well-known institutions. Once compromised, these assets are repurposed for scams, malware delivery, and fraudulent traffic campaigns. This tactic damages both the end users and the reputation of the organizations whose names are used. It reflects a broader issue: **digital infrastructure that isn't maintained doesn't just pose internal risk—it becomes a liability to the broader internet ecosystem**.

Third-party software continues to present risk as well. A recent flaw in **Microsoft's OneDrive File Picker** revealed that selecting a single document could grant access to an entire user drive, depending on how OAuth permissions were configured. This kind of overreach isn't always visible to security teams, especially when it happens within platforms managed by external vendors. It highlights a persistent challenge in SaaS security: visibility and control are limited, but responsibility remains with the organization.

These incidents share a common thread: small oversights—unmonitored credentials, outdated links, or vague consent settings—are enabling larger compromises. Security failures are no longer isolated to individual systems. A weak control in one place can create opportunities for exploitation across partners, customers, and shared platforms. Preventing this will require stronger lifecycle management, better collaboration between teams, and a more disciplined approach to maintaining the digital environment.

RETURN

Executive Overview

DR AS A TARGET

LAPSES IN IT HYGIENE

Audience
- C-Suite Executives
- CISO
- IT Managers
- Risk Management Professionals
- Cybersecurity Professionals
- Developers

Since December 2023, the threat actor known as Hazy Hawk has exploited abandoned cloud resources–primarily misconfigured DNS CNAME records pointing to expired cloud services such as Amazon S3 buckets and Azure endpoints–to hijack domains tied to high-trust organizations. These hijacked subdomains are then used to distribute scams, ad-fraud schemes, and push-notification based malware. Victim organizations include the CDC, the Australian Department of Health, University of California at Berkeley, and firms like Deloitte and PwC. This operation not only endangers users but also severely tarnishes the reputation of compromised entities, highlighting a broader issue of organizational neglect in DNS and asset hygiene.

READ MORE: LAPSES IN IT HYGIENE

NON-HUMAN INTERVENTION

Audience
- CISO
- C-Suite Executives
- Risk Management Professionals
- IT Managers
- Cybersecurity Analysts
- Project Managers

Non-human identities have emerged as the modern enterprise's most exploitable weak point. As attackers pivot away from targeting human credentials, they are leveraging unmanaged API keys, OAuth tokens, and service accounts to infiltrate trusted systems, pivot laterally, and persist undetected. With these credentials now outnumbering human accounts by as much as 50:1, traditional identity controls are being routinely bypassed. Organizations that fail to bring visibility, governance, and lifecycle control to NHIs face systemic and escalating supply chain risk.

READ MORE: NON-HUMAN INTERVENTION

TO MANY CONNECTIONS, TOO LITTLE CONTROL

Audience
- CISO
- Risk Management Professionals
- Security Managers
- Cybersecurity Professionals
- Project Managers

A critical security design flaw in Microsoft's OneDrive File Picker allows integrated SaaS applications to access the entire contents of a user's OneDrive, even when a single file is selected. This flaw, caused by coarse OAuth permissions and vague consent language, affects hundreds of applications and millions of users. The incident demonstrates how third-party SaaS tools embedded within enterprise ecosystems can bypass security boundaries without triggering traditional controls. Organizations must be operationally prepared to respond when these issues arise in platforms they do not own or fully manage.

READ MORE: TO MANY CONNECTIONS

RETURN

LAPSES IN IT HYGIENE

OVERVIEW & IMPACT

The Hazy Hawk campaign highlights the consequences of poor DNS hygiene and unmanaged cloud assets. By targeting misconfigured DNS CNAME records pointing to decommissioned cloud services, threat actors gained control over domains belonging to reputable organizations. These domains were then used to distribute scams, malicious push notifications, and fraudulent content, often through traffic distribution systems (TDS).

This activity demonstrates how insufficient lifecycle management of digital infrastructure can inadvertently support threat operations. The failure of one organization to secure its digital assets can directly impact others, making IT hygiene a collective security responsibility across sectors.

- **Brand and Trust Degradation:** Compromised domains, including those of public health agencies and multinational firms, were repurposed to serve malicious content, undermining institutional credibility.
- **Massive Campaign Reach via TDS:** Hijacked subdomains were embedded into TDS chains, facilitating large-scale scam and malware distribution globally.
- **Persistent Victim Targeting:** Users tricked into enabling browser notifications were repeatedly exposed to fraudulent advertisements and scams.
- **Monetization Through Affiliate Abuse:** Threat actors leveraged advertising affiliate networks for financial gain, amplifying the impact of each hijacked domain.
- **Governance Breakdown in Cloud Asset Management:** The use of abandoned S3 buckets, Azure endpoints, and other cloud services revealed widespread asset mismanagement.
- **Collateral Exposure Across the Ecosystem:** Single points of DNS failure contributed to broader campaign scalability, affecting external users and partners.
- **Detection Avoidance:** Multi-layered obfuscation and redirection techniques hindered traditional detection and response tools.

OBSERVATIONS

- The actor hijacked subdomains from domains including cdc.gov, health.gov.au, berkeley.edu, and ey.com.
- Attack infrastructure spans Amazon S3, Azure Web Apps, GitHub, Netlify, and CDNs like Akamai and Cloudflare.
- Malicious content delivery leverages multi-stage redirection paths and traffic distribution systems (TDS).
- Push notification abuse serves as a persistent attack vector, even post initial compromise.

RETURN

GUIDANCE

Strategic Intelligence

- **Trend**
  - Rising exploitation of abandoned cloud assets and misconfigured DNS as low-effort, high-impact vectors in affiliate ad-fraud and phishing ecosystems.
- **Strategic Insight**
  - Lapses in DNS hygiene contribute to a secondary victimization pattern, where trusted domains are weaponized for broader scam operations.
  - As organizations increasingly adopt cloud-first models, asset visibility and lifecycle governance become pivotal in defending digital trust and operational integrity.
  - Industry-wide DNS negligence directly empowers adversaries. A coordinated effort toward better hygiene reduces attacker opportunities and limits the blast radius of individual oversights.

Operational Intelligence

- **Threat Vectors**
  - Dangling DNS CNAME records pointing to decommissioned services (e.g., Azure endpoints, S3 buckets).
  - Open redirection via abandoned or unmonitored domains.
  - Exploited subdomains on public developer platforms like GitHub and Netlify.
- **Monitoring & Detection Gaps**
  - Lack of lifecycle management for DNS entries tied to ephemeral or test cloud environments.
  - Insufficient passive DNS telemetry to detect hijacks.
  - Inconsistent enforcement of DNS hygiene policies across departments or subsidiaries.
- **Response Actions**
  - Immediately audit and remove obsolete DNS CNAME records linked to decommissioned services.
  - Monitor subdomain traffic for anomalous redirects or adtech indicators.
  - Integrate passive DNS and cloud asset inventory tools into the security stack.

Tactical Intelligence

- **Mitigation Strategies**
  - Use automated tools to identify and remediate dangling DNS records.
  - Enforce mandatory DNS hygiene reviews during project shutdowns or M&A integrations.
  - Implement least privilege access to DNS management interfaces to prevent unauthorized changes.
- **Preventive Measures**
  - Deploy DNS security solutions with TDS detection capabilities.
  - Educate users to deny browser notification prompts from unknown domains.
  - Adopt digital asset management platforms that inventory and track all DNS and cloud resources.

RETURN

THREAT HUNTING HYPOTHESES

Subdomain Hijack via Abandoned DNS Records

Hypothesis: Hazy Hawk hijacked subdomains of our organization via dangling DNS CNAME records.

Investigation Steps:

- Query historical passive DNS data for subdomains pointing to external cloud providers.
- Identify and resolve NXDOMAIN responses for CNAME targets.
- Investigate DNS changes post-service decommissioning.
- Look for suspicious traffic spikes from browser push notifications or adtech domains.

User Redirection via Threat Actor-Controlled Infrastructure

Hypothesis: Users in our environment are being redirected through Hazy Hawk-controlled TDS chains.

Investigation Steps:

- Monitor DNS and HTTP logs for domains such as viralclipnow[.]xyz, chesta-korci-bro[.]blogspot[.]com, and others mentioned in Infoblox IOCs.
- Investigate browser push notification subscription requests from compromised domains.
- Cross-reference URL redirection paths with known affiliate ad-fraud infrastructure.

Sources

- **HackRead:** Hazy Hawk Attack Exploits Abandoned Cloud Assets Since 2023
- **Infoblox:** Cloudy with a Chance of Hijacking - Forgotten DNS Records Enable Scam Actor
- **The Hacker News:** Hazy Hawk Exploits DNS Records to Hijack Reputable Domains
- **Dark Reading:** Hazy Hawk Cybercrime Gang Abuses Cloud Resources in Sophisticated Scam
- **SecurityBrief UK:** Hazy Hawk Exploits Abandoned Cloud DNS for Global Scams Surge
- **SC World:** Misconfigured DNS, Neglected Cloud Assets Harnessed in Hazy Hawk Domain Hijacking Attacks

NON-HUMAN INTERVENTION

OVERVIEW & IMPACT

Recent campaigns demonstrate a paradigm shift in attacker methodology, targeting programmatic access pathways rather than user credentials. NHIs are typically generated for internal automation or third-party integrations, yet many persist with excessive permissions, lack expiration controls, and are invisible to IAM governance. Vaulting practices are inconsistent, and secrets are frequently exposed across code repositories, collaboration tools, and messaging platforms. Once compromised, NHIs offer attackers direct, persistent access to critical cloud assets.

- **Impact**
  - Persistent access to enterprise systems via exposed or unrotated API keys and OAuth tokens
  - Lateral movement across cloud services using compromised machine credentials
  - Exploited shadow IT integrations and unauthorized third-party access

OBSERVATIONS

- Overprivileged OAuth apps used in Microsoft and GitHub breaches
- Exposed service accounts enabled persistent attacker access in Cloudflare
- Gitloker and HuggingFace exploited API tokens to access and manipulate codebases
- 91% of former employee tokens remain active and exploitable

GUIDANCE

Strategic Intelligence

- **Trend**
  - Adversaries increasingly exploiting non-human identities over human credentials for persistent access
  - Mismanagement of NHI lifecycle is driving a new generation of supply chain attacks, bypassing traditional IAM controls
- **Contextual Insight**
  - NHIs now comprise the majority of digital identities in enterprise environments, often exceeding human identities by a factor of 50-90:1, creating a threat landscape that is vast, dynamic, and opaque.
  - The proliferation of low-code/no-code and AI-powered platforms is accelerating the creation of NHIs outside security purview, compounding governance challenges.
  - Regulatory frameworks such as GDPR, HIPAA, and PCI-DSS increasingly view NHI security as within scope, elevating compliance risk for organizations that lack structured NHI controls.
- **Investment Priorities**
  - NHI-focused solutions (e.g., posture management, usage-based access control, anomaly detection for NHIs) should be prioritized alongside IAM modernization efforts.
  - Boards and executive leadership must treat NHI governance as a strategic initiative equivalent in importance to human identity management.
- **Agentic AI Acceleration Risk**
  - Agentic AI systems generate dynamic, autonomous, and context-sensitive access demands, creating non-deterministic NHI behavior.

RETURN

- Traditional monitoring and policy enforcement mechanisms cannot adequately address AI-generated or delegated credentials, increasing the risk of undetected privilege escalation and exfiltration.

- **Third-Party Exposure Amplification:**
  - The average employee connects 10+ third-party tools to core systems; each integration creates NHIs with varying levels of access.
  - Vendors' security controls often fall short of internal standards, yet NHIs connected through these apps inherit trust relationships with core environments (e.g., GitHub, Salesforce, Microsoft 365).

Operational Intelligence

- **Threat Vectors**
  - NHI tokens leaked via public code repositories, configuration missteps, or messaging platforms.
  - OAuth abuse and malicious third-party app integrations.
- **Monitoring & Detection Gaps**
  - Lack of centralized NHI inventory, real-time visibility, or behavioral baselining.
  - Absence of context-aware secret management and anomaly detection tools.
- **Response Actions**
  - Immediate revocation of unused or untracked NHI credentials; accelerate adoption of automated NHI discovery and governance

- **Control Validation**
  - Conduct periodic red-teaming or purple-teaming exercises targeting NHI misuse scenarios
  - Simulate compromise of high-impact NHIs to evaluate detection and containment speed
  - Review vault misconfiguration reports to identify secrets lacking encryption or access policies
- **Tooling Recommendations:**
  - Deploy specialized NHI posture management solutions that integrate with IAM and SIEM platforms
  - Integrate automated secrets scanning into CI/CD pipelines and source code management platforms
  - Use NHIDR (Non-Human Identity Detection and Response) tools to correlate NHI behavior with threat models

Tactical Intelligence

- **Mitigation Strategies**
  - Enforce least privilege for all NHIs.
  - Automate secret rotation and vault enforcement policies.
  - Block unauthorized OAuth apps and monitor usage patterns.

- **Preventive Measures**
  - Deploy lifecycle controls for creation, classification, and decommissioning of NHIs.
  - Map and eliminate unused or duplicative tokens.
  - Mandate approval workflows and visibility for all app integrations.

RETURN

THREAT HUNTING HYPOTHESES

Undetected OAuth Token Abuse

Hypothesis: OAuth tokens granted to third-party apps were not rotated and have been used to exfiltrate data.

Investigation Steps:

- Review all OAuth grants for high-privilege scopes (e.g., repo access, admin privileges).
- Analyze access logs for token usage from unrecognized IPs, devices, or geographies.
- Check app registration metadata for suspicious or inactive developers.
- Correlate token use with spikes in data transfers or unauthorized actions.
- Confirm abuse if data exfiltration aligns with token activity patterns.

Stale Service Accounts Enabling Lateral Movement

Hypothesis: Orphaned service accounts with elevated permissions are active in the environment.

Investigation Steps:

- Identify service accounts with no interactive logins or recent activity but with valid credentials.
- Cross-reference authentication logs to confirm inactivity and permissions scope.
- Map access rights to validate potential lateral movement paths.
- Investigate whether the accounts are still tied to any live processes or scripts.
- Confirm the risk by identifying unused accounts with privileged access.

Exposed Secrets in Collaboration Tools

Hypothesis: Sensitive API keys or secrets have been shared in Slack, Jira, or Confluence.

Investigation Steps:

- Audit code repositories (e.g., GitHub, Bitbucket) using secret detection tools.
- Review commit history for token-like patterns using regex.
- Compare usage timestamps with repository commit times.
- Analyze authentication logs for token usage from abnormal IPs or geographies.
- Success is defined by confirmed use of leaked tokens to access systems.

Tactical Guidance

Shadow App Integrations via Unauthorized OAuth

Hypothesis: OAuth apps registered by unknown actors are siphoning data via trusted access.

Investigation Steps:

- Inventory all OAuth applications across tenants; flag unverified or inactive developers.
- Identify apps granted elevated scopes without proper approvals.
- Correlate usage patterns with data access anomalies.
- Pivot from token usage to API logs to track data queries or exfiltration attempts.
- Confirm compromise if unauthorized apps show persistent or privileged access patterns.

Exposed Secrets in Collaboration Tools

Hypothesis: Sensitive API keys or secrets have been shared in Slack, Jira, or Confluence.

Investigation Steps:

- Run regex-based scans across chat, ticketing, and documentation platforms for common secret formats (e.g., AWS keys, JWTs).
- Cross-reference discovered secrets with vault entries or source code for validation.
- Check message metadata for unauthorized sharing of credentials.
- Map exposure to access events or privilege misuse.
- Confirm incident if any discovered secrets were actively used during the exposure window.

Sources

- **Astrix:** 11 Attacks in 13 Months
- **Entro Security:** 2025 NHI & Secrets Report
- **CrowdStrike:** NHI Management Guide
- **The Hacker News:** The Hidden Threat in Your Stack
- **Oleria:** Solving the NHI Crisis
- **Dark Reading:** NHIs Gain Momentum
- **Security Magazine:** Managing the Invisible Risk
- **Cybersecurity Tribe:** Addressing the Blindspot
- **Cyber Defense Magazine:** 20% Breached

TO MANY CONNECTIONS, TOO LITTLE CONTROL

OVERVIEW & IMPACT

The core issue with Microsoft's OneDrive File Picker—broad OAuth scopes combined with vague user consent flows—exemplifies a category of SaaS design flaws that pose significant risk to enterprises. This is not an isolated Microsoft-specific failure; similar models exist across many SaaS platforms where identity delegation and third-party integrations are key features.

OAuth-based authorization, while standardized, is inconsistently implemented across vendors. In many cases, the default scopes requested by third-party applications exceed operational necessity. Because consent interfaces are designed for speed and simplicity rather than risk clarity, users frequently approve integrations without understanding that doing so may grant persistent, organization-wide access to sensitive resources.

In environments where SaaS products are managed outside of centralized IT or IAM processes—such as through shadow IT, unsanctioned plug-ins, or delegated admin privileges—these integrations may never be reviewed, scoped, or logged. This creates operational blind spots where enterprises do not possess the authority, visibility, or telemetry to detect or contain data exfiltration risks. Even when issues are disclosed, vendors may classify them as "expected behavior" or "configuration issues," thereby limiting response options.

- **SaaS Scope Misalignment:** Third-party integrations across platforms like Google Workspace, Dropbox, Zoom, Slack, and Salesforce may request overly broad scopes under default OAuth implementations, leading to excessive data exposure.
- **Vendor-Controlled Boundaries:** Enterprises relying on external SaaS products have limited leverage to enforce secure defaults or initiate immediate changes when flaws are discovered. If the vendor does not treat the issue as a vulnerability, the organization may be left unprotected.
- **Lack of Incident Ownership:** Incidents stemming from misused OAuth grants may fall into a response gray zone—neither fully internal nor clearly attributable to malicious behavior. This complicates attribution, forensics, and regulatory reporting.
- **Delayed Detection and Escalation:** Without telemetry into the authorization lifecycle (e.g., consent event logs, token re-use tracking), security teams may be unaware of exploit conditions until data loss or unusual activity is discovered via downstream effects.
- **Compliance and Legal Uncertainty:** Depending on regional laws, exposure of user data through "consented" third-party access may still trigger reporting requirements—particularly if consent was obtained under misleading pretenses.

OBSERVATIONS

- Microsoft's File Picker defaults to Files.ReadWrite.All, regardless of user intent.
- Hundreds of integrated SaaS apps are implicated, from productivity tools to AI services.
- Consent screens do not inform users of full-drive access.
- Tokens remain active in session/local storage and may be extended using refresh workflows.
- Microsoft has not provided timeline for fine-grained scope implementation.

GUIDANCE

Strategic Intelligence

- **Trend**
  - OAuth and token-based authorizations are becoming prime exposure points across SaaS ecosystems, often exploited unintentionally due to poor defaults.
- **Cross-SaaS Relevance**
  - This is not limited to OneDrive. Any SaaS product using embedded identity providers, file pickers, or federated access may suffer similar over-scoping risks. Platforms like Google Workspace, Dropbox, Salesforce, Zoom, and even GitHub allow third-party integrations with significant access capabilities that can be under-examined.
- **CISO-Level Insight**
  - Security teams cannot rely solely on vendor assurances or assume least-privilege by default. Instead, organizations need processes to audit third-party access continuously, enforce granular scopes via conditional policies, and integrate scope-based risk scoring into vendor evaluations.
- **Strategic Readiness Gap**
  - SaaS security strategies must evolve from static configuration reviews to dynamic control and detection frameworks that anticipate vendor-origin vulnerabilities. This includes identifying what tooling is required to log, detect, and respond to consent-based access scenarios that do not involve malware or exploits.

Operational Intelligence

- **Threat Vectors**
  - OAuth-based integrations with excessive permission requests across SaaS environments.
- **Monitoring & Detection Gaps**
  - Absence of delegated scope visibility across non-Microsoft SaaS platforms.
  - Inability to trace downstream data access once OAuth tokens are granted.
  - Lack of correlation between user intent and token permissions granted.
- **Response Actions**
  - Revoke or reauthorize applications with known overbroad scopes.
  - Mandate approval workflows for high-risk SaaS integrations.
  - Shorten access token lifespans and prohibit persistent refresh tokens.
  - Disable embedded File Picker tools or equivalents when safer alternatives are unavailable.

RETURN

Tactical Intelligence

- **Mitigation Strategies**
  - Use Entra or equivalent IAM systems to enforce scope constraints.
  - Disable or gate integrations using broad OAuth scopes (Files.ReadWrite.All, Mail.ReadWrite, etc.).
  - Enable tenant-wide auditing and enforce admin consent policies.
- **Preventive Measures**
  - Deploy SaaS Security Posture Management (SSPM) tools to map OAuth grants across platforms.
  - Educate users on scope implications and visible consent UX.
  - Run quarterly reviews of SaaS integrations and their granted permissions using identity governance tools.

THREAT HUNTING HYPOTHESES

Over-Permissioned SaaS Integrations

Hypothesis: Broad OAuth permissions granted to third-party SaaS apps beyond intended use

Investigation Steps:

- Aggregate OAuth scope grants across SaaS apps (Microsoft 365, Google Workspace, Salesforce, etc.).
- Search for applications using Files.Read.All, Mail.ReadWrite, Drive.ReadWrite, or similar high-privilege scopes.
- Correlate scope grants with user/app behaviors (e.g., single file uploads vs. drive-wide access).
- Identify apps without centralized approval or outside policy.

Persistent and Unsecured Token Storage

Hypothesis: Persisting access tokens in client-side storage

Investigation Steps:

- Analyze endpoint/browser telemetry (e.g., EDR browser extensions) for access token presence in sessionStorage/localStorage.
- Compare token lifespan against organizational policies.
- Trace token re-use after user logout or session expiration.

Scope Misuse in API Access Patterns

Hypothesis: Unexpected API access patterns in integrated SaaS apps

Investigation Steps:

- Collect Graph API logs (Microsoft) or Admin SDK logs (Google).
- Filter for apps making directory-wide or bulk data retrieval calls.
- Identify access events from apps expected to perform single actions.
- Look for off-hours or geographically anomalous access.

RETURN

Consent Discrepancy Detection

Hypothesis: Other SaaS ecosystems suffer similar consent UX flaws

Investigation Steps:

- Review and screenshot consent dialogs across Google, Dropbox, Salesforce, and others.
- Map scope-to-permission correlation (what is being asked vs. what is granted).
- Interview sample users to assess understanding of granted access.

Orphaned Tokens with Residual Access

Hypothesis: Orphaned OAuth tokens retain unmonitored access

Investigation Steps:

- Query OAuth token activity logs for deactivated users or dormant apps.
- Identify tokens issued to unused accounts, service principals, or SaaS tools no longer in use.
- Look for token refresh or access activity post user termination or project decommission.

Scope Escalation After Initial Authorization

Hypothesis: SaaS apps reauthorize for broader scopes post-deployment

Investigation Steps:

- Analyze consent history to detect scope changes for previously authorized applications.
- Compare initial granted scopes vs. current permissions.
- Investigate app behavior post-escalation for broader data access.

Success Criteria:

- Apps expanding privileges beyond original user or admin approval.

Misaligned Session and Token Expiry Policies

Hypothesis: OAuth tokens outlive session boundaries across SaaS platforms

Investigation Steps:

- Compare session termination logs to token expiration and refresh activity.
- Review SaaS token policies to determine if logout events trigger revocation.
- Audit for continued token usage after session ends.

Tactical Guidance

Sources

- **Oasis Security:** OneDrive File Picker Flaw
- **Secure-ISS Advisory**
- **The Hacker News**
- **SecureWorld**
- **Infosecurity Magazine**

CONVERGE
TECHNOLOGY SOLUTIONS

Contact the Converge Threat Intel Group at cybersecurity@convergetp.com

convergetp.com/cybersecurity