ARTEX / Exposed Secrets

Microsoft links GitHub scanning for secrets to ARTEX; in a follow-on attack, app credentials of unresolved origin reached Key Vault, SharePoint and MSPs' clients, per Microsoft and Todyl.

Reflects the csoh.org kill chain as of 2026-11-21

Cloud Security Office Hours, csoh.org

Slides licensed CC BY-NC 4.0

How to use this deck

Read it on your own or present it. Every fact about the incident comes from the csoh.org kill chain and the sources it cites.

Slides marked Background explain a general idea and name their own source. The speaker notes are a presenter's script.

Full kill chain: csoh.org/breaches/artex-github-secrets-azure.html. These slides reflect it as of 2026-11-21.

At a glance

Dozens

apps with successful service principal sign-ins

across multiple tenants, per Microsoft

33+

of about 45 targeted apps authenticated

in Todyl's telemetry, at about 18 organizations

27

organizations reached through those apps

including MSPs' clients, per Todyl, which calls it a floor

Microsoft names no actor. Todyl assesses the activity as unrelated to the Storm-0940 ConnectWise compromise.

What happened, and when

August 2026
Microsoft starts observing GitHub queries for secrets

October 28
Microsoft's earliest reported successful sign-ins

November 1
Todyl first sees the main address

November 3
Detections fire; Todyl sees every token replay blocked

November 5
Microsoft publishes its account

November 6
Todyl's update calls it AI-driven tooling

Microsoft names no actor. Where the credentials came from is unresolved. The page gives no end date. Spacing is not to scale.

Where the credentials came from is unresolved

Todyl, November 3	Todyl, November 6
• Origin unknown • Read secret pairs as pointing to a file store or live backend • A tampered Claude Code extension: plausible, tied to no affected organization	• An agentic credential crawler • Read Microsoft's GitHub finding as confirmation • Does not address its November 3 evidence

Microsoft leans toward GitHub but, for sign-ins from October 28, says only leaked or stolen. Todyl's reading goes further than Microsoft does.

Agent or person? The accounts read it differently

Todyl, November 3	Todyl, November 6
• Its telemetry did not show an AI model directing the activity • Read idle gaps and a switch to spoofed browser signatures as a person steering • Held AI direction at low confidence	• AI-driven tooling acting with little human direction • Lists the switch to spoofed browser user agents as crawler behavior • Does not revisit the idle gaps or its earlier low confidence

Microsoft's published evidence for agents is speed and API retries, and nothing it publishes separates an agent from a script or an operator.

Where ARTEX is named, and where it is not

Where	What it says
Microsoft, summary	The actors used ARTEX to search GitHub for OAuth app secrets
Microsoft, body	An agentic AI offensive framework; ARTEX is an example of such tooling
Microsoft, sign-ins	Only "an agentic framework"
Microsoft, detections	Unattributed ARTEX-related network indicators, not published
Todyl, November 6	Writes that Microsoft names the tooling as ARTEX

Todyl's claim goes beyond Microsoft's post. Microsoft does not say how it identified the framework, and it names no actor.

The kill chain on one slide

01
Reconnaissance
GitHub secret queries
T1593.003

02
Initial Access
Signing in as the workload
T1078.004

03
Credential Access
Resource Manager then Key Vault
T1555.006

04
Discovery
Mapping Azure
T1580

05
Collection
Files and mailbox items
T1213.002

06
Initial Access
From the MSP to its clients
T1199

07
Lateral Movement
Beyond app secrets
T1550.001

08
Impact
AI keys and the bill
T1496.004

Arrows show order only; the page leaves open where stage 02's credentials came from.

01 Large volumes of GitHub queries for secrets

T1593.003 Search Open Websites/Domains: Code Repositories

Since	August 2026, per Microsoft
Query terms	target name, secret keywords, a cloud or AI provider keyword
Sought	credentials, application credentials, AI inference API keys
Tooling	an agentic framework that Microsoft links to ARTEX

WHY IT MATTERS

Microsoft says removing a leaked secret does not invalidate it or erase its copies in edit history, caches, archives and logs.

02 Signing in as service principals

T1078.004 Valid Accounts: Cloud Accounts

Window	as early as October 28 (Microsoft); November 1 to 3 (Todyl)
Microsoft	successful sign-ins on dozens of apps across multiple tenants
Targeted (Todyl)	about 45 apps at about 18 organizations; 33+ authenticated
Credential origin	unresolved

WHY IT MATTERS

An app sign-in raises no MFA prompt, and Conditional Access scoped to users does not apply to it, as Todyl points out.

BACKGROUND

What an app registration and a service principal are

Registering an app creates one application object, in its home tenant. A service principal is the app's instance in each tenant where it is used, and it defines what the app can do there.

Source: Microsoft Learn, application and service principal objects (learn.microsoft.com)

03 Tokens for Resource Manager, then Key Vault

T1555.006 Credentials from Password Stores: Cloud Secrets Management Stores

Token order (Todyl)	Resource Manager, then Key Vault, often then Graph and others
Microsoft	targeted storage keys, connection strings, AKS user credentials
Connector (Todyl)	archive downloaded, its app signed in about 2.5 minutes later
Microsoft, one case	GitHub search to Key Vault exfiltration in five minutes

WHY IT MATTERS

Previously unused apps authenticated within minutes. Todyl says the timing suggests Key Vault reads were one source; Key Vault audit logs are needed to confirm it.

04 Mapping Azure, and correcting its own calls

T1580 Cloud Infrastructure Discovery

Mapped (Microsoft)	subscriptions, resource groups, permissions, AI deployments
Key Vault metadata	HTTP 400; about 28 s later, API version 2023-07-01, HTTP 200
SQL firewall rules	HTTP 400; about 60 s later, only api-version changed, HTTP 200
Third example	an Application Insights query, about 80 s apart

> **WHY IT MATTERS**
>
> With the five-minute case, these are Microsoft's most specific evidence for agents; it publishes nothing that separates an agent from a script or an operator.

BACKGROUND

Azure’s control plane and data plane

The control plane manages resources in a subscription; every request goes to Azure Resource Manager, whose APIs require an api-version parameter. The data plane uses what a resource instance exposes, like a storage account's data, at its own endpoint.

Source: Microsoft Learn, Azure control plane and data plane (learn.microsoft.com)
Also from the Azure REST API reference, and Secure your Azure Key Vault (learn.microsoft.com)

05 Files named pass, key and access

T1213.002 Data from Information Repositories: Sharepoint

Searches (Todyl)	29 wildcard Graph searches across about 25 tenants
Downloads (Todyl)	81 at about one a second, favoring names like pass, key, access
Mail items (Todyl)	about 2,279 accessed
Not seen (Todyl)	extortion demand, encryption or destruction

WHY IT MATTERS

Per Todyl, the files held password lists, private keys and VPN profiles. It expects their use against systems it cannot see from Microsoft 365 logs.

06 MSP apps carried access into client tenants

T1199 Trusted Relationship

One app	15 client tenants in about 10-second loops (Todyl)
Partner Center	a token obtained by one MSP's app (Todyl)
GDAP	automation app tried against clients, without success (Todyl)
Vendor apps	a multitenant credential compromised at the source (Microsoft)

WHY IT MATTERS

Security tools' integration apps were among those abused, including Todyl's own in two MSP tenants. Todyl says there is no sign any vendor platform was compromised.

BACKGROUND

What GDAP gives a Microsoft partner

Granular delegated admin privileges (GDAP), set up through Partner Center, give a Microsoft partner granular, time-bound access to a customer's workloads. The customer must explicitly grant that least-privileged access.

Source: Microsoft Learn, introduction to GDAP (learn.microsoft.com)
Also from GDAP frequently asked questions (learn.microsoft.com)

07 Azure DevOps, replayed tokens and Run Command

T1550.001 Use Alternate Authentication Material: Application Access Token

Azure DevOps	federated identity used; two users' sessions replayed (Todyl)
VMs	Run Command called through a compromised OAuth app (Microsoft)
Refresh tokens	replayed November 3, all blocked by Conditional Access (Todyl)
Persistence	none seen by Todyl

WHY IT MATTERS

Todyl warns that rotation is not enough on its own: the actor kept retrying disabled and rotated apps and moved on to replaying users' refresh tokens.

BACKGROUND

What workload identity federation does

Workload identity federation lets an app registration or user-assigned managed identity trust tokens from an external identity provider. The workload trades that provider's token for a Microsoft access token, with no secret to manage.

Source: Microsoft Learn, workload identity federation concepts (learn.microsoft.com)

08 AI service keys, and one partner’s bill

T1496.004 Resource Hijacking: Cloud Service Hijacking

Focus (Microsoft)	AI provider API keys and apps with Foundry Tools access
Tokens (Todyl)	four AI-service tokens at two MSPs, which do not prove use
Billing (Todyl)	thousands of dollars in about 10 minutes, one partner
Motive (Todyl)	fits an initial access broker or LLM access resale

WHY IT MATTERS

Microsoft says the actor attempted to validate stolen Azure resources, including compromised Azure AI services, and might have attempted to abuse some of them.

BACKGROUND

What ATT&CK calls Cloud Service Hijacking

Adversaries may use compromised software-as-a-service applications for resource-intensive tasks, such as mass spam or, in LLMjacking, hijacking cloud-hosted AI models. The victim may face significant costs, used-up service quotas and other effects on availability.

Source: MITRE ATT&CK T1496.004 (attack.mitre.org)

Six defenses against eight stages

	01	02	03	04	05	06	07	08
Rotate secrets that reached a public repository	●							
Contain the app in Microsoft's order		●	●		●		●	●
Conditional Access for workload identities, plus a user block		●					●	
Hunt back to at least October 28		●	●					
Retire client secrets, protect the issuer, fence Key Vault and Storage		●	●				●	
MSPs audit partner apps and GDAP						●		

No defense on the page is tied to stage 04, the discovery and API retries.

Rotate exposed secrets, and contain the app

Rotate exposed secrets

- Treat a secret in a public repository as compromised
- Removing it does not invalidate it, per Microsoft
- Secret scanning with public monitoring, and push protection
- Todyl: stop AI agents using or posting cleartext secrets

Contain the app

- Remove every client secret, certificate and federated credential
- Disable it if needed; issued tokens stay valid until expiry
- Rotate Key Vaults it could read, and credentials in documents it accessed
- Todyl adds: rotate AI keys, review billing

Microsoft: revoke affected users' Entra sessions, Azure DevOps PATs and SSH keys.

Block app sign-ins with a policy for workload identities

What to do	Its limits
• Policies scoped to users miss app sign-ins; target workload identities • Microsoft: block 199.19.77[.]84/32, plus a user-scoped block for replays • Todyl: require a compliant device or trusted location	• Needs Workload ID Premium; single-tenant apps in your tenant only • Not managed identities, multitenant apps or third-party SaaS (Todyl) • The app that swept 15 client tenants was multi-tenant

The sources differ on scope: Microsoft says block the exact IP, not the ASN; Todyl's November 6 update recommends 199.19.77[.]0/24 and 65.87.223[.]26.

Retire client secrets; MSPs audit partner apps and GDAP

Retire client secrets

- Managed identities first, then federation, then certificates (Todyl)
- Todyl: app policies that block new secrets and cap lifetimes
- Todyl: federation trusts the issuer, here Azure DevOps; protect it
- Key Vault and Storage on selected networks or private endpoints

If you are an MSP

- Review Partner Center access, GDAP and customer tenants
- Notify affected customers under your agreements
- Todyl: least-privilege, time-bound GDAP
- Todyl: no customer app secrets in runbooks, notes or client documents

Addresses to hunt, and what each source says

Address	Microsoft	Todyl
199.19.77[.]84	a main source of sign-ins	every confirmed sign-in, download, replay
199.19.77[.]18	a main source; Tor exit node	spraying, probing; low to moderate confidence
65.87.223[.]26	potentially associated	same spraying, October 4 to 27; all failed
157.22.126[.]128	AI workload reconnaissance	-
Three Microsoft IPs	-	the actor's searches and mail reads appear under them; do not block

Both sources expect the infrastructure to change; hunt the behavior too.

Hunt the behavior, and count the failures

Sign-in logs	Behavior
• Service principal and non-interactive sign-ins, back to at least October 28 • Include failures, as far back as retention allows • AADSTS7000215 or AADSTS7000222: someone holds your app's credential • A failure followed by a success is urgent	• One address, three or more service principals, mixed success • One app: Resource Manager, Key Vault, Storage and Graph tokens in a short window • A Resource Manager token, then Key Vault, then unused apps signing in within minutes

Actor-unique client fingerprints (Todyl): task177-f2267/1.0, sait-tenant-deep/37346.

Check your own environment

- [ ] Was every secret that reached a public repository rotated, not only removed?
- [ ] Do you use secret scanning with public monitoring, and push protection?
- [ ] Does a Conditional Access policy target your workload identities, not only your users?
- [ ] Would you notice failed client-secret sign-ins to your apps, followed by a success?
- [ ] Which of your apps still use client secrets rather than managed identities or federation?
- [ ] Can any address with a valid token reach your Key Vaults and Storage?
- [ ] If you are an MSP, when did you last review GDAP relationships?

DISCUSSION

You rotated the leaked secret. Are you done?

Suppose one of your apps' client secrets leaked and you rotated it.

Using what the page reports, what could still go wrong, and what would you check next?

DISCUSSION: ANSWER

Rotation alone is not enough, per the page

The page gives three reasons.

- Issued tokens stay valid until they expire.
- Todyl: the actor retried disabled and rotated apps, then replayed users' refresh tokens.
- Target workload identities with Conditional Access; rotate what the app could read.

DISCUSSION

What would you add for stage 04?

No page defense is tied to stage 04, where a client retried failed Resource Manager calls with corrected API versions within 28 to 80 seconds.

What would you watch for, and what would it catch?

DISCUSSION: ANSWER

The page ties no defense to stage 04

Any control you propose is your own suggestion. Test it against the reported details: HTTP 400 followed by HTTP 200 after a corrected API version, and enumeration of subscriptions, permissions and AI deployments.

Sources

Microsoft, agentic AI tooling and exposed secrets
microsoft.com

Todyl, Stolen App Credentials, Real Access (updated November 6)
todyl.com

MITRE ATT&CK T1593.003
attack.mitre.org/techniques/T1593/003

MITRE ATT&CK T1078.004
attack.mitre.org/techniques/T1078/004

MITRE ATT&CK T1555.006
attack.mitre.org/techniques/T1555/006

MITRE ATT&CK T1199
attack.mitre.org/techniques/T1199

Related kill chains

ARTEX also appears in both. Todyl assesses this activity as unrelated to the ConnectWise Cloud Backup compromise attributed to Storm-0940.

VAPOR PANDA / ARTEX
csoh.org/breaches/vapor-panda-artex.html

Storm-0940 and ConnectWise
csoh.org/breaches/storm-0940-connectwise.html

Read the full kill chain

Every step, source and defense in detail:
https://csoh.org/breaches/artex-github-secrets-azure.html

Cloud Security Office Hours, csoh.org. Slides licensed CC BY-NC 4.0 (creativecommons.org/licenses/by-nc/4.0). Third-party excerpts keep their own licenses.