ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Passkey-Themed Social Engineering Campaign Targeting Cloud Identities and SaaS Data

TLP: CLEAR
Distribution: Public
Advisory on: Passkey-Themed Social Engineering Campaign Targeting Cloud Identities and SaaS Data
Severity: High
Threat Type: Identity Compromise / Social Engineering / AiTM Phishing / Cloud Account Takeover
Potentially Affected Sectors: Government, financial services, telecommunications, energy, healthcare, education, technology, manufacturing, defense, critical infrastructure and other organizations using cloud identity platforms
Primary Platform: Cloud identities, Microsoft 365/Entra ID environments, SaaS applications
Date: 14 September 2026

Executive Summary

BGD e-GOV CIRT is issuing this advisory regarding an active social-engineering campaign in which threat actors use **passkey, MFA, SSO and identity-verification themes to compromise cloud identities and subsequently access organizational cloud resources**.

The campaign is particularly significant because the passkey itself is **not the vulnerability**. Instead, threat actors use the promise of passkey enrollment or MFA configuration as a social-engineering pretext. Victims may receive a phone call or message from an individual impersonating an internal IT/helpdesk employee and are instructed to complete an urgent authentication or passkey-registration process. The victim is then redirected to an attacker-controlled authentication page or instructed to complete a legitimate device-code authentication process.

Microsoft has observed multiple attack paths involving **adversary-in-the-middle (AiTM) phishing, device-code phishing, stolen session/token replay, and previously registered attacker-controlled MFA methods**. Following successful identity compromise, actors register their own authentication method, conduct Microsoft Graph reconnaissance, enumerate users, groups, roles, applications, SharePoint/OneDrive repositories and mailboxes, and subsequently perform sustained collection of cloud-hosted files and email.

The campaign demonstrates a shift from conventional endpoint-centric intrusion toward **identity-centric cloud compromise**. No malware installation or traditional network lateral movement is necessarily required. A compromised cloud identity can provide direct access to email, documents, collaboration platforms and other SaaS applications.

Microsoft reports that the activity has been observed since May 2026 and assesses that the initial-access activity is used by multiple threat actors, including clusters tracked as **Storm-3121** and **Storm-3032**, among others. Attribution should therefore not be generalized to a single actor.

Threat Overview

The campaign follows an identity-to-cloud attack lifecycle:

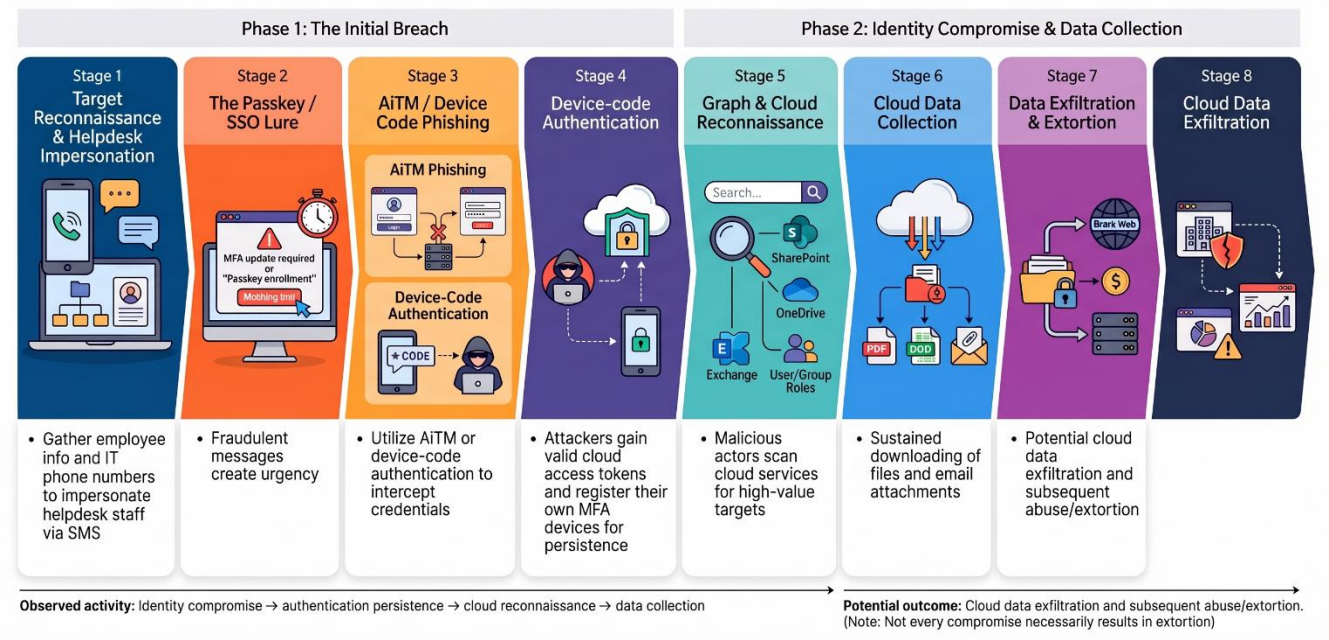

Figure: Passkey-Themed Social Engineering to Cloud Identity Compromise and Data Collection

Microsoft's observed sequence specifically links unusual sign-ins with new authentication-method registration, Graph reconnaissance, SharePoint/OneDrive access and email collection.

Significance of the Campaign

Traditional phishing investigations frequently focus on:

- malicious URLs;
- malicious attachments;
- endpoint malware;
- suspicious processes;
- command-and-control infrastructure.

This campaign can bypass much of that visibility. A successful attack may involve:

- A phone call to the victim's personal number.
- An SMS or collaboration message.
- A browser session.
- A legitimate cloud authentication page.
- A legitimate authentication token.
- A legitimate cloud identity.
- Legitimate cloud APIs.

Consequently, **endpoint malware may never be installed**.

When a victim uses a personal mobile device that is not covered by enterprise endpoint telemetry, the initial phishing interaction may produce little or no endpoint evidence. The victim's recollection of the phone call or message may become an important initial forensic clue.

Initial Access — Passkey-Themed Social Engineering

Helpdesk impersonation:

The attack commonly begins with an attacker impersonating:

- IT helpdesk personnel;
- identity-management personnel;
- system administrators;
- security teams;
- technical support staff.

The victim is told that an authentication-related change is urgently required. Common pretexts include:

- *Passkey enrollment required*
- *MFA migration required*
- *SSO configuration update*
- *Account verification required*
- *Authentication synchronization required*
- *Security registration required*

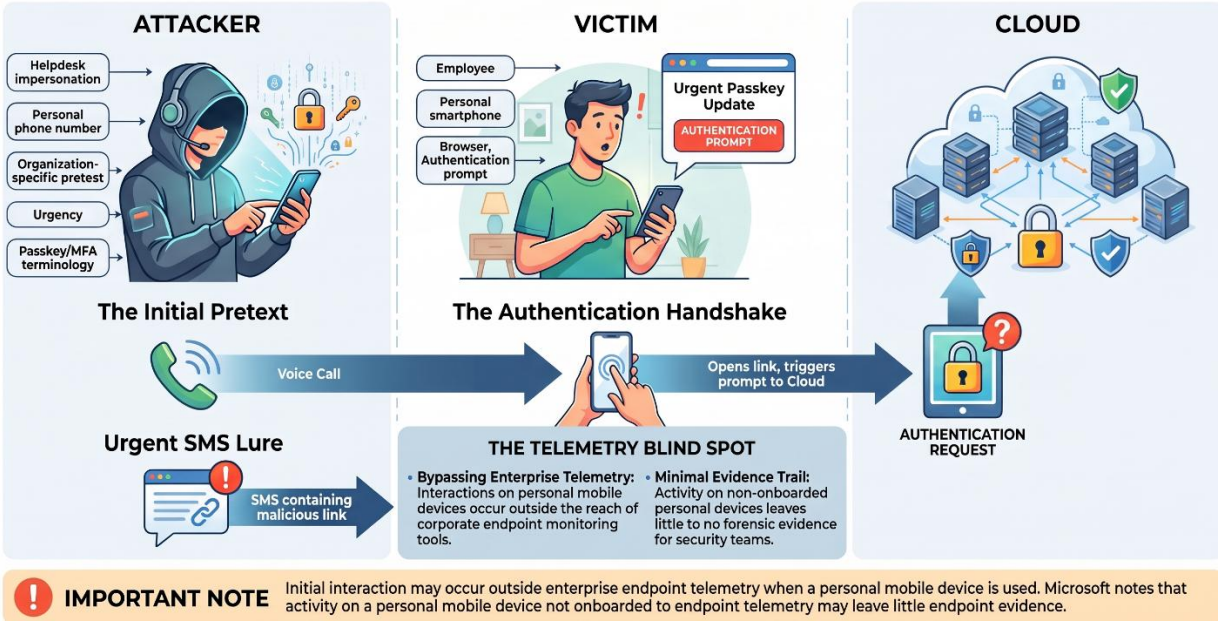

Figure: Passkey-Themed Social Engineering and Helpdesk Impersonation

The objective is to make the victim believe that **authentication itself is the problem that must be fixed**. In reality, the authentication workflow is the attack surface.

Personal phone numbers as an attack channel:

A notable characteristic is the use of employees' personal phone numbers. This creates a serious visibility problem for enterprise SOC teams because the initial interaction may occur completely outside organizational infrastructure.

Organization-Specific Phishing Infrastructure

Threat actors have used rapidly created domains that incorporate the target organization's name into the URL structure. For example:

- `<organization-name>.add-passkey[.]com`
- `<organization-name>.secure-passkey[.]com`
- `<organization-name>.integratedsso[.]com`

The purpose is to make the URL appear organization-specific even though the actual registered domain is controlled by the attacker.

Observed themes include:

Theme	Example domains
Passkey support	`passkeyhelpdesk[.]com`
Passkey security	`secure-passkey[.]com`
Passkey setup	`setupmypasskey[.]com`
Passkey enrollment	`add-passkey[.]com`
SSO	`integratedsso[.]com`
Identity provider	`oktasession[.]com`
Key synchronization	`keysyncos[.]com`
Key setup	`oskeysetup[.]com`
Key registration	`oskeyregister[.]com`
Key synchronization	`syncmykey[.]com`
Key connection	`myconnectkey[.]com`
Validation	`validationsetupac[.]com`
Portal setup	`portalsetuphub[.]com`

These indicators should be treated as **campaign-specific IOCs**, not permanent blocking signatures. Microsoft warns that domains and infrastructure can change rapidly.

Adversary-in-the-Middle Authentication

One observed path uses AiTM phishing. The victim believes they are authenticating to the organization's legitimate cloud service. Conceptually:

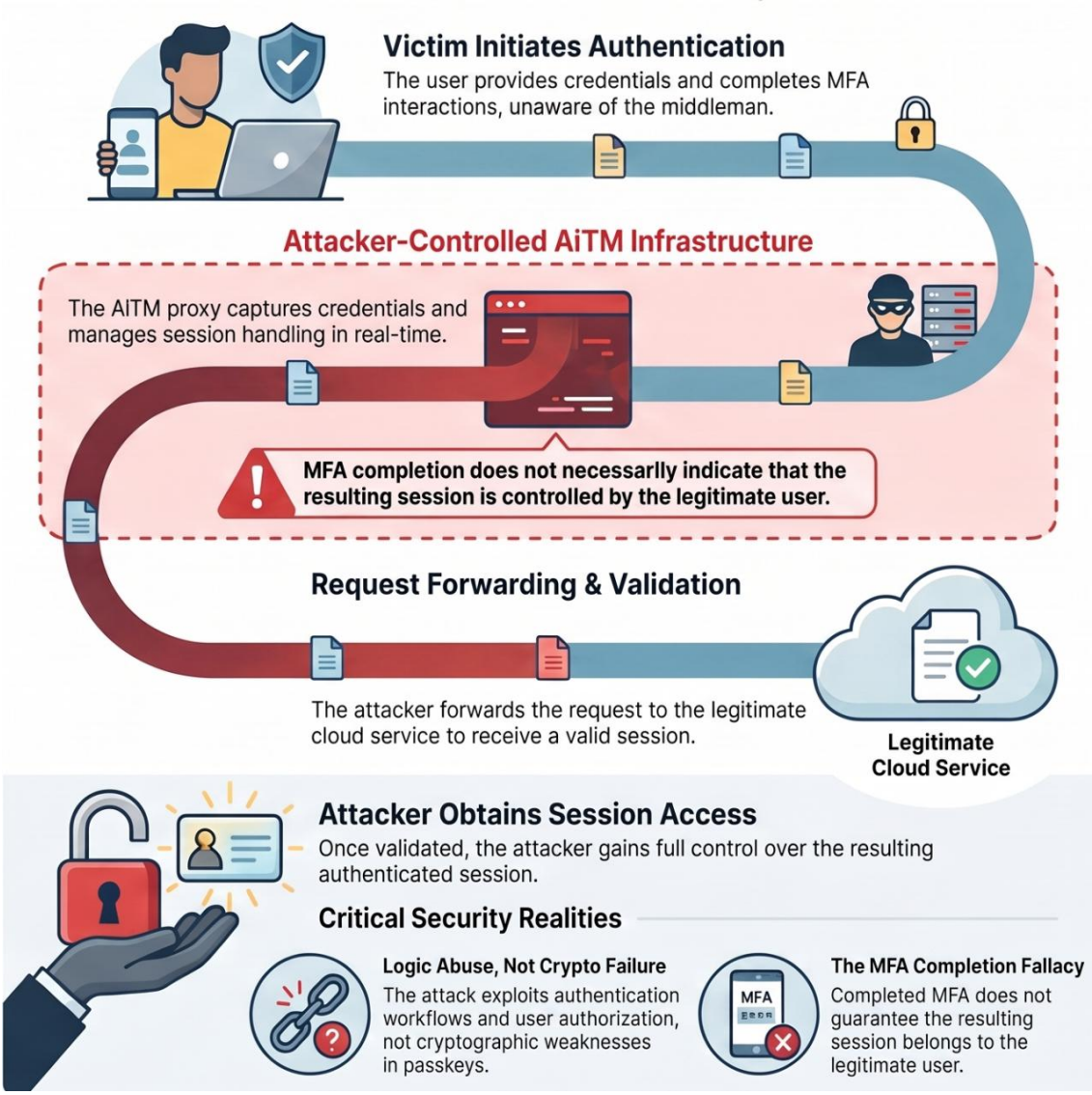

Figure: Adversary-in-the-Middle Authentication Flow

The important distinction is that the victim may actually complete MFA successfully.

Therefore:

"**MFA succeeded" does not necessarily mean "the legitimate user is operating the session**."

In the observed activity, Microsoft identified authentication sequences consistent with AiTM involving non-phishing-resistant MFA.

Device-Code Phishing

A second major technique is **device-code authentication abuse**. The victim may be instructed to enter an authentication code into a legitimate cloud authentication page. The victim believes: "I am completing the requested passkey/MFA setup."

However, the code may have been generated by an attacker-controlled authentication process. The resulting flow can be represented as:

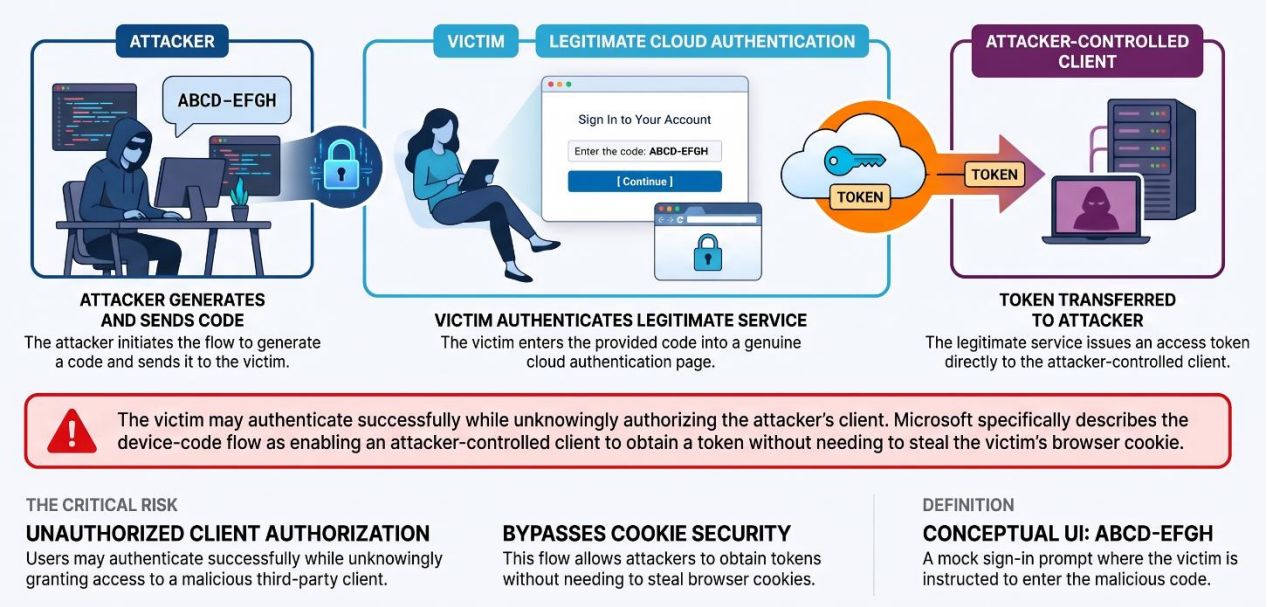

Figure: Device-Code Phishing (Victim Authorizes an Attacker-Controlled Client)

It has been observed in a case where the attacker used the device-code flow to compromise a session token and subsequently replayed the token to progress through reconnaissance and further activity.

Identity Compromise

After successful authentication, the attacker may access multiple cloud applications using the compromised identity. An observed sequence included:(The sequence can occur rapidly)

- OfficeHome;
- My Apps;
- My Profile;
- My Sign-Ins;
- Microsoft Approval Management;
- SharePoint Online;
- OneDrive;

- Outlook Web;
- Microsoft 365 collaboration services;
- other internal applications.

In one observed timeline:

- T+0 Anomalous OfficeHome authentication
- T+1m MFA completed
- T+1m Cloud session established
- T+2m Application enumeration
- T+2m Profile information accessed
- T+3m Approval-management services accessed
- T+4m Sign-in/security information accessed
- T+10m Application catalogue accessed
- T+11m+ SharePoint / Outlook activity

This demonstrates why **post-authentication behavior is as important as the initial authentication event .**

Attacker-Controlled MFA Persistence

One of the most important stages is the registration of a new authentication method. The attacker may register:

- a new phone number;
- an authenticator application;
- a software-based OTP token;
- another authentication device.

This converts a temporary account compromise into a more persistent identity foothold.

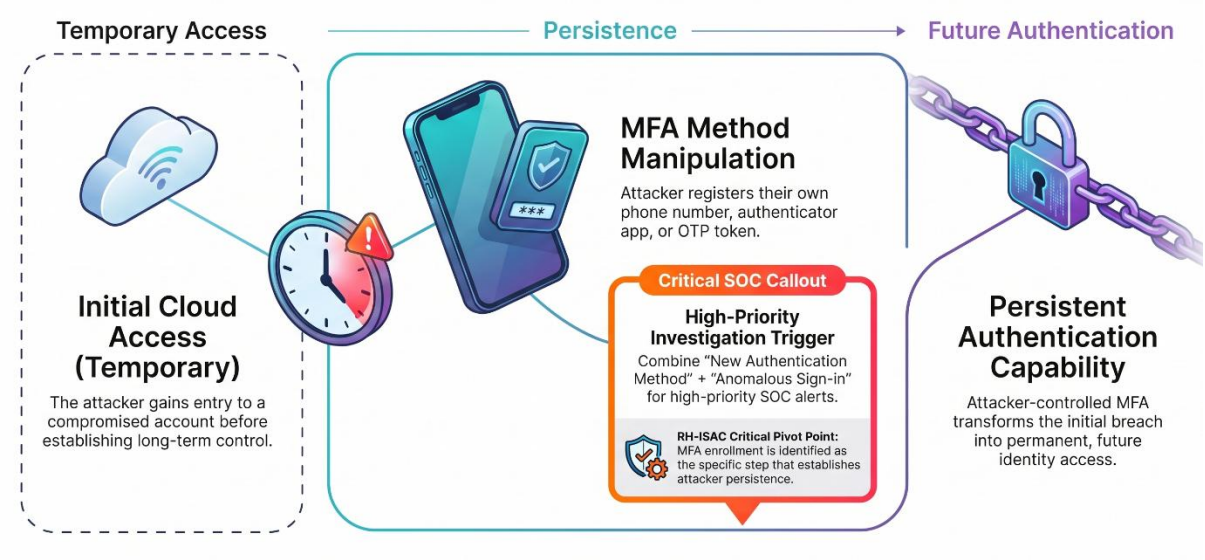

Figure: Conversion of Temporary Account Compromise into Persistent Identity Access

Microsoft Graph Reconnaissance

Once persistence is established, the attacker can use Microsoft Graph to understand the tenant. Graph activity is particularly challenging because individual API requests may appear legitimate. For example:

- `/users`
- `/groups`
- `/sites`
- `/drives`
- `/messages`

are normal enterprise operations. The malicious signal emerges from **sequence, breadth, identity, source and timing**.

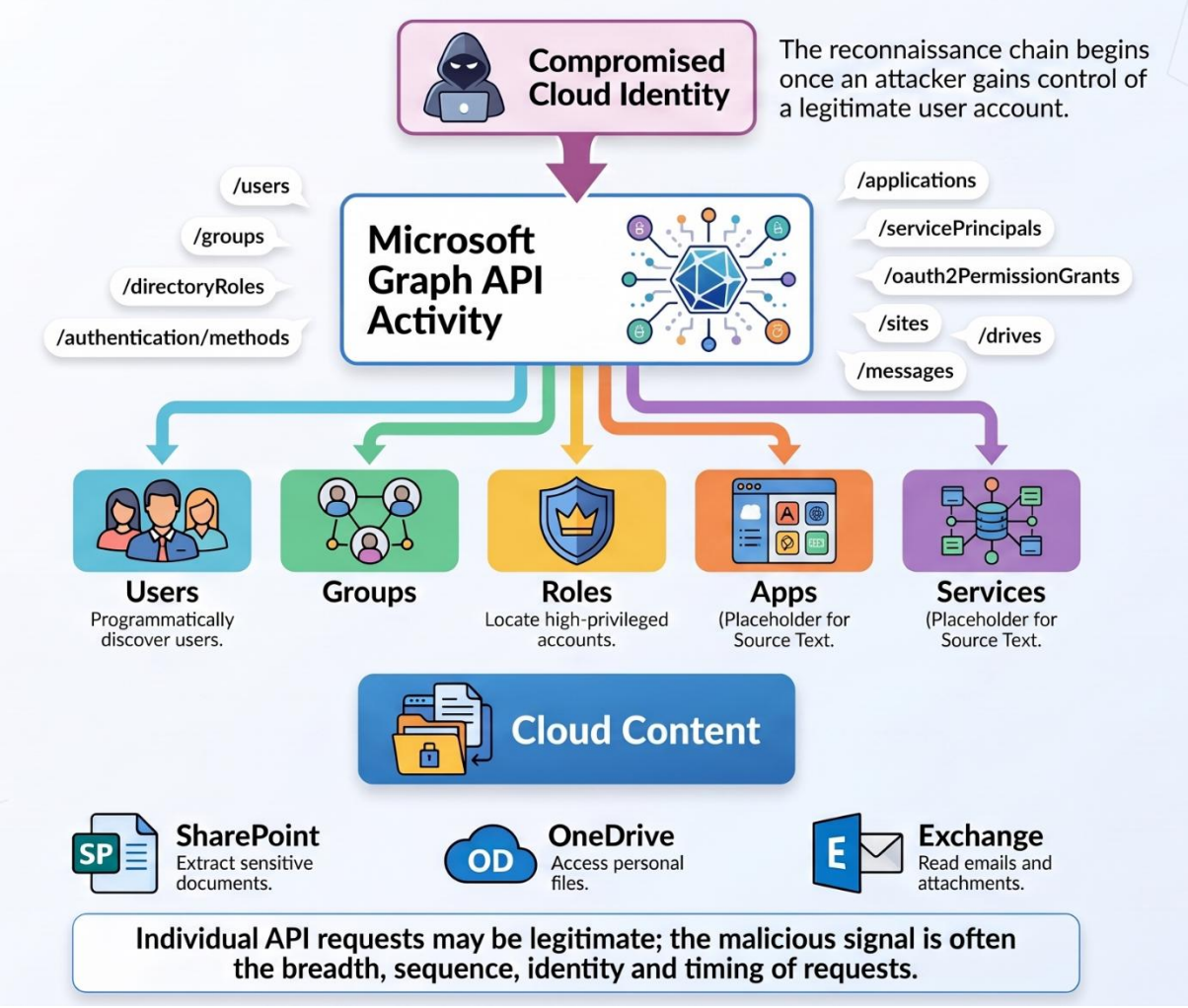

Figure: Microsoft Graph as the Cloud Reconnaissance Plane

Tenant discovery

Observed reconnaissance can include:

- `/organization`

- `/subscribedSkus`
- `/licenseDetails`

These can reveal:

- tenant identity;
- verified domains;
- enabled services;
- licensing;
- cloud-service footprint.

Directory enumeration

Observed paths include:

- `/users`
- `/groups`
- `/members`
- `/transitiveMembers`

These can help an attacker identify:

- users;
- groups;
- privileged identities;
- organizational relationships;
- high-value personnel.

Privilege and MFA discovery

Observed paths include:

- `/directoryRoles`
- `/roleManagement`
- `/authentication/methods`

These are especially important because they can expose the organization's identity-control structure.

Application and OAuth discovery

Observed paths include:

- `/applications`
- `/servicePrincipals`
- `/oauth2PermissionGrants`
- `/appRoleAssignments`

These can expose:

- enterprise applications;
- service principals;
- delegated permissions;
- application permissions;
- reusable access paths.

SharePoint and OneDrive discovery

Observed paths include:

- `/sites`
- `/lists`
- `/drives`
- `/drive/items`
- `/root/children`
- `/search`

The attacker may additionally use: (to systematically traverse large repositories)

- `$top`
- `$skip`
- `$skiptoken`
- `$delta`
- `/search`

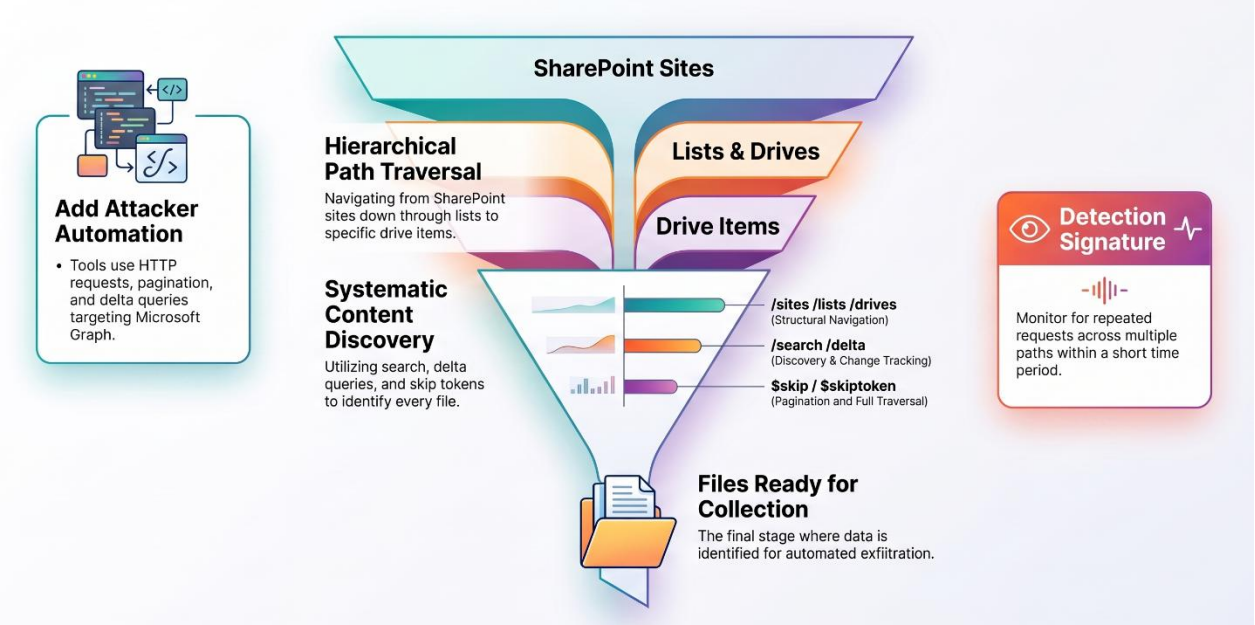

Figure: Automated SharePoint and OneDrive Repository Enumeration

Mailbox Reconnaissance

The campaign also targets email. Observed Graph resources include:

- `/messages`
- `/mailFolders`
- `/attachments`

This allows attackers to search:

- business correspondence;
- attachments;
- organizational information;
- credentials or secrets accidentally transmitted by email;
- financial information;
- internal documents;
- operational information.

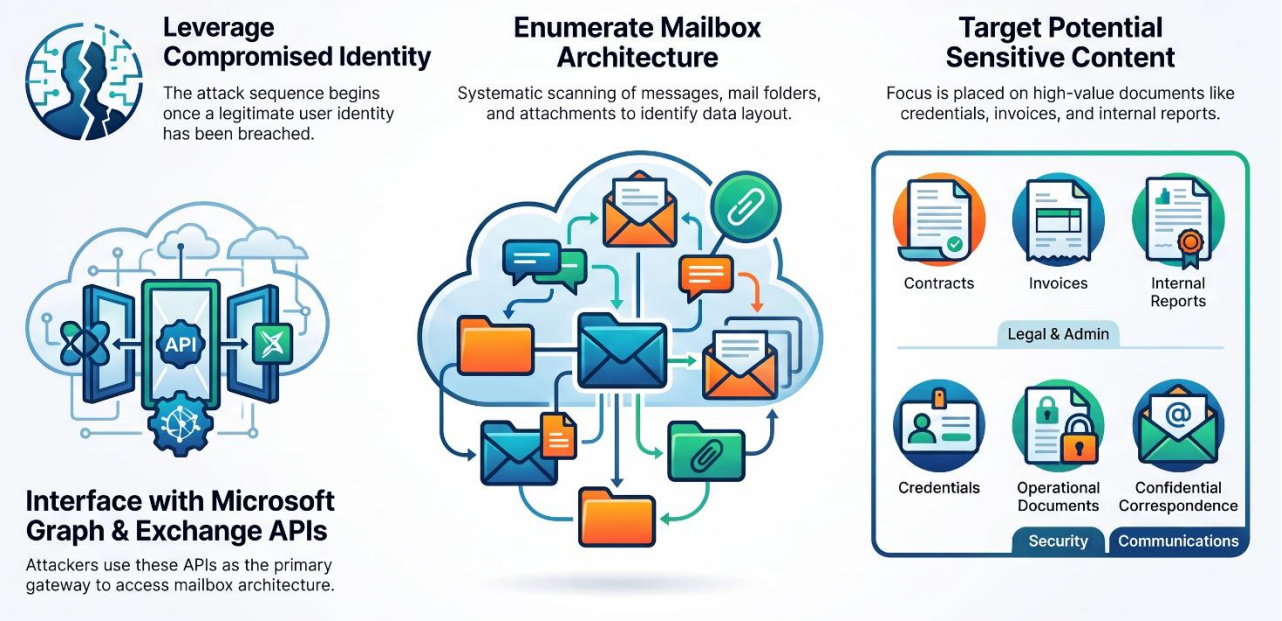

Figure: Cloud Mailbox Enumeration and Email Collection

The combination of mailbox discovery and attachment retrieval is substantially more concerning than isolated mailbox access.

Cloud Data Collection

After reconnaissance, the attack transitions into systematic collection. Primary targets include:

- SharePoint;
- OneDrive;
- Exchange Online;

- organizational document repositories;
- email attachments.

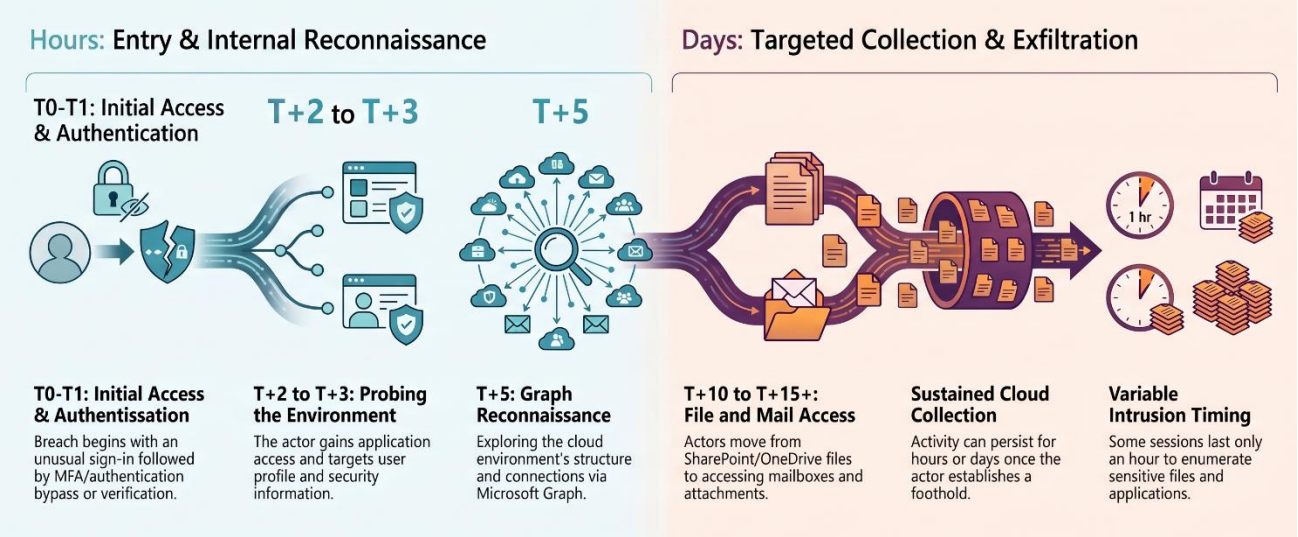

Figure: Observed Identity-to-Cloud Data Collection Progression

Microsoft observed high volumes of:

- `FileAccessed`;
- `FileDownloaded`;
- `SyncDownloadedFull`.

The activity frequently exhibited automation characteristics. In several cases, the python-httpx user agent appeared in high-volume SharePoint/OneDrive activity.

However: `python-httpx` **alone should NOT be treated as a malicious IOC.** It should be correlated with:

- compromised identity;
- unusual IP/ISP;
- anonymous proxy use;
- abnormal data volume;
- Graph reconnaissance;
- newly registered MFA;
- unusual application activity

Low-and-Slow Cloud Exfiltration

An important characteristic is that collection may not be extremely fast. Microsoft observed activity lasting:

- several hours;
- multiple days;

with actors generally maintaining a controlled collection rate. In observed cases, fewer than approximately **1,000 files or emails per hour** could be accessed while still enabling significant aggregate collection over time.

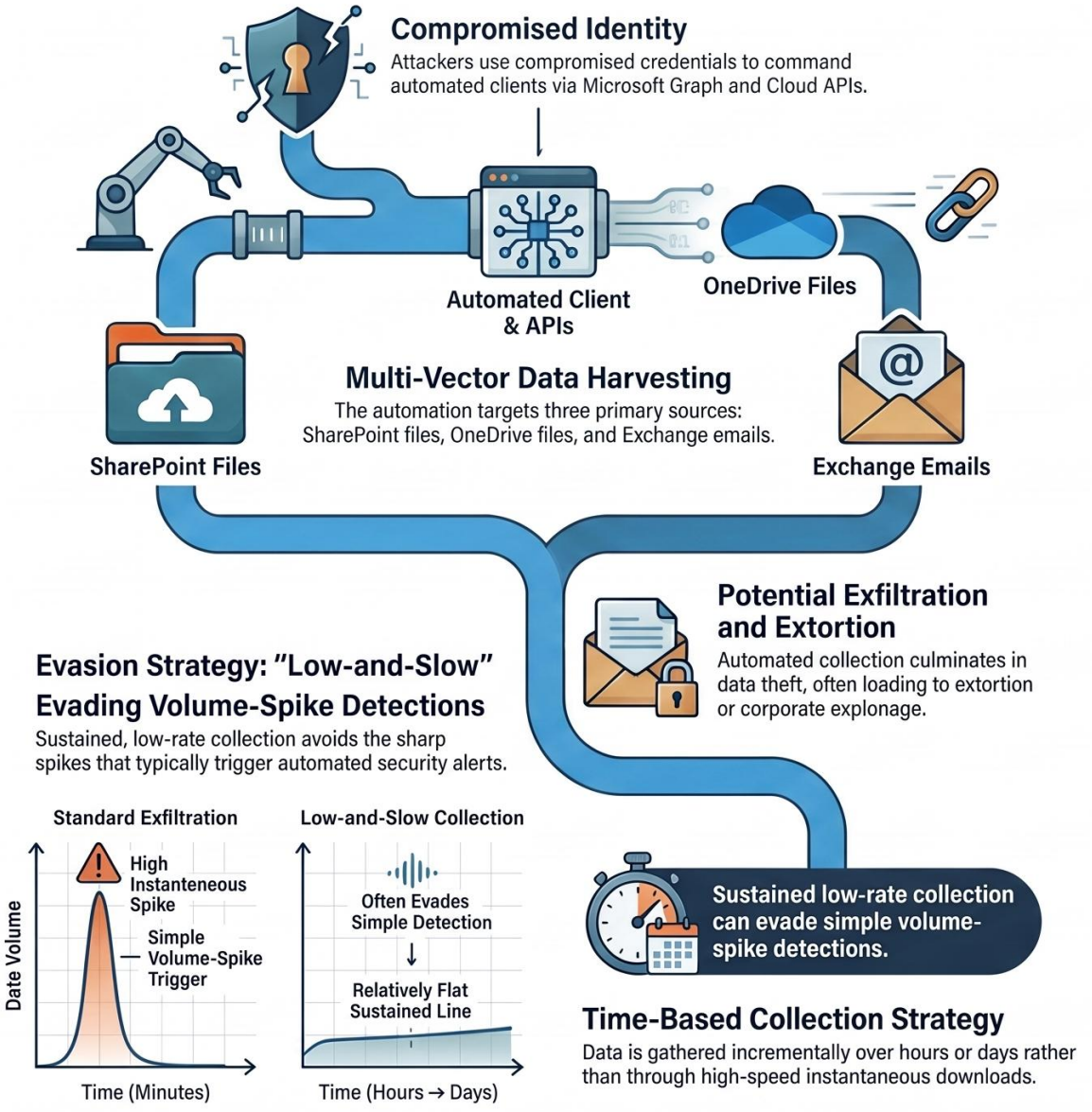

Figure: Automated Cloud Data Collection and Potential Exfiltration

This means conventional alerts such as: "**Very large number of downloads in five minutes**" may fail to detect the activity. Organizations should instead baseline:

- per-user file access;
- per-user download behavior;
- application usage;
- source network;
- geographical location;
- ISP;

- user-agent;
- repository breadth;
- API request patterns.

MITRE ATT&CK Mapping

Tactic	Technique	ID	Observed/Relevant Activity
Reconnaissance	Gather Victim Organization Information	**T1591**	Research of employees and organization
Reconnaissance	Phishing for Information: Spearphishing Link	**T1598.003**	Authentication-themed phishing links
Resource Development	Acquire Infrastructure: Domains	**T1583.001**	Registration of phishing domains
Resource Development	Establish Accounts: Email Accounts	**T1585.002**	Supporting delivery infrastructure
Initial Access	Valid Accounts: Cloud Accounts	**T1078.004**	Use of compromised cloud identity
Persistence	Modify Authentication Process: MFA	**T1556.006**	Attacker-controlled MFA registration
Discovery	Account Discovery: Cloud Account	**T1087.004**	Graph-based user enumeration
Discovery	Permission Groups Discovery: Cloud Groups	**T1069.003**	Group/role enumeration
Collection	Data from Cloud Storage	**T1530**	SharePoint/OneDrive collection
Collection	Email Collection	**T1114**	Mailbox/message/attachment collection
Collection	Data from Information Repositories	**T1213**	Cloud repository discovery and collection
Exfiltration	Exfiltration Over Web Service	**T1567**	Cloud-based data collection/exfiltration

Indicators of Compromise (IoC)

Campaign Domains

Indicator	Type	Description
passkeyhelpdesk[.]com	Domain	Passkey/helpdesk-themed social-engineering lure
secure-passkey[.]com	Domain	Passkey security-themed lure
setupmypasskey[.]com	Domain	Passkey setup/enrollment lure
add-passkey[.]com	Domain	Passkey enrollment lure
integratedsso[.]com	Domain	SSO/integrated authentication-themed lure
oktasession[.]com	Domain	Identity-provider/session-themed lure
keysyncos[.]com	Domain	Key synchronization-themed lure
oskeysync[.]com	Domain	Key synchronization-themed lure
oskeysetup[.]com	Domain	Security-key/passkey setup-themed lure
oskeyregister[.]com	Domain	Security-key/passkey registration-themed lure
syncmykey[.]com	Domain	Key synchronization-themed lure
myconnectkey[.]com	Domain	Key connection/authentication-themed lure
oskeyconnect[.]com	Domain	Security-key/passkey connection-themed lure
validationsetupac[.]com	Domain	Account validation/setup-themed lure
portalsetuphub[.]com	Domain	Authentication/portal setup-themed lure

Indicators of Attack / Behavioral Indicators

For this particular campaign, **IoAs are more valuable than the domains alone**.

Behavioral Indicator	Type	Detection Relevance
Unexpected phone call claiming to be IT/helpdesk	Social Engineering	Possible initial-access precursor
Unsolicited passkey/MFA enrollment request	Social Engineering	Strong campaign-context indicator
Device-code authentication initiated after helpdesk contact	Authentication	High-risk identity event
Successful authentication from unusual device/location	Identity	Potential compromised session
New MFA/authentication method registered shortly after unusual sign-in	Persistence	High-priority compromise indicator
Rapid Graph enumeration of users and groups	Cloud Discovery	Possible tenant reconnaissance
Access to `/directoryRoles` or authentication methods	Privilege/Identity Discovery	Possible privilege mapping
Enumeration of applications/service principals/OAuth grants	Cloud Discovery	Possible application/permission reconnaissance

Rapid `/sites` and `/drives` enumeration	Cloud Discovery	Possible SharePoint/OneDrive discovery
Repeated `$skiptoken`, `$delta`, `/search`, or pagination requests	Automated Discovery	Possible automated repository traversal
Unusual `/messages` and `/attachments` activity	Collection	Possible mailbox collection
Sustained `FileAccessed` / `FileDownloaded` activity	Collection	Possible cloud data collection
`python-httpx` **associated with anomalous cloud access**	User-Agent / Behavioral	Supporting indicator only; not malicious by itself
Anonymous/residential proxy + abnormal cloud downloads	Network/Identity	Elevated compromise confidence

Detection and Monitoring

Highest-priority correlation

SOC teams should prioritize the following sequence; The presence of multiple stages should significantly increase confidence.

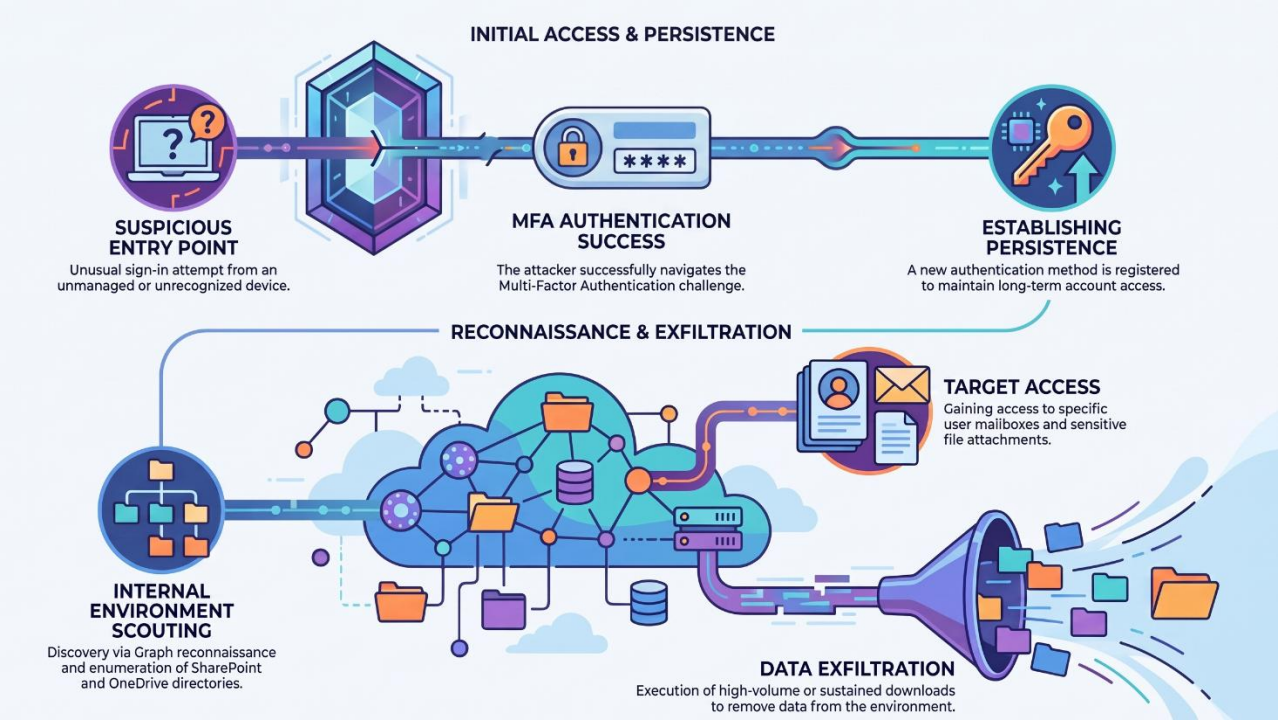

Figure: SOC team Correlation sequence

Authentication monitoring

Alert on:

- new MFA device;

- new phone MFA;
- new authenticator;
- new software OTP;
- sign-in from unusual location;
- sign-in from unfamiliar ISP;
- sign-in from anonymous/residential proxy;
- authentication immediately followed by broad cloud access;
- device-code authentication where not normally required.

Figure: Identity-to-Cloud Detection and Correlation Architecture

Graph API Detection

Monitor for identities or applications accessing multiple reconnaissance categories within a short period. High-value URI groups include:

- `/organization`
- `/subscribedSkus`
- `/users`
- `/groups`
- `/directoryRoles`
- `/roleManagement`
- `/authentication/methods`
- `/applications`
- `/servicePrincipals`
- `/oauth2PermissionGrants`
- `/appRoleAssignments`
- `/sites`
- `/drives`
- `/messages`
- `/mailFolders`
- `/attachments`

Microsoft provides a hunting approach using approximately 30-minute windows, with thresholds such as multiple reconnaissance categories and multiple distinct paths.

SharePoint / OneDrive Detection

Monitor: (for automated repository traversal)

- `/sites`
- `/drives`
- `/drive/`
- `/search`
- `/children`
- `/delta`
- `$skiptoken`
- `$top`

Microsoft's example hunting logic identifies:

- ≥8 requests;
- ≥4 distinct paths;
- within approximately 20 minutes;

when associated with repository discovery patterns. These values should be tuned against each organization's normal baseline rather than treated as universal thresholds.

Mailbox Detection

Monitor:

- `/messages`
- `/mailFolders`
- `/attachments`

and correlate:

- number of requests;
- distinct paths;
- attachment requests;
- response size;
- source IP;
- user-agent;
- identity risk.

Microsoft's example identifies concentrated mailbox reconnaissance using request and path thresholds and separately considers attachment requests

Cloud Exfiltration Detection

- Signal A — Automated file access
- Signal B — Anonymous proxy

Microsoft's example considers approximately:

- ≥5 GB within a two-hour bucket, or
- ≥1,000 events,

as a hunting threshold. These are detection heuristics, not universal maliciousness thresholds.

SIEM Correlation Model

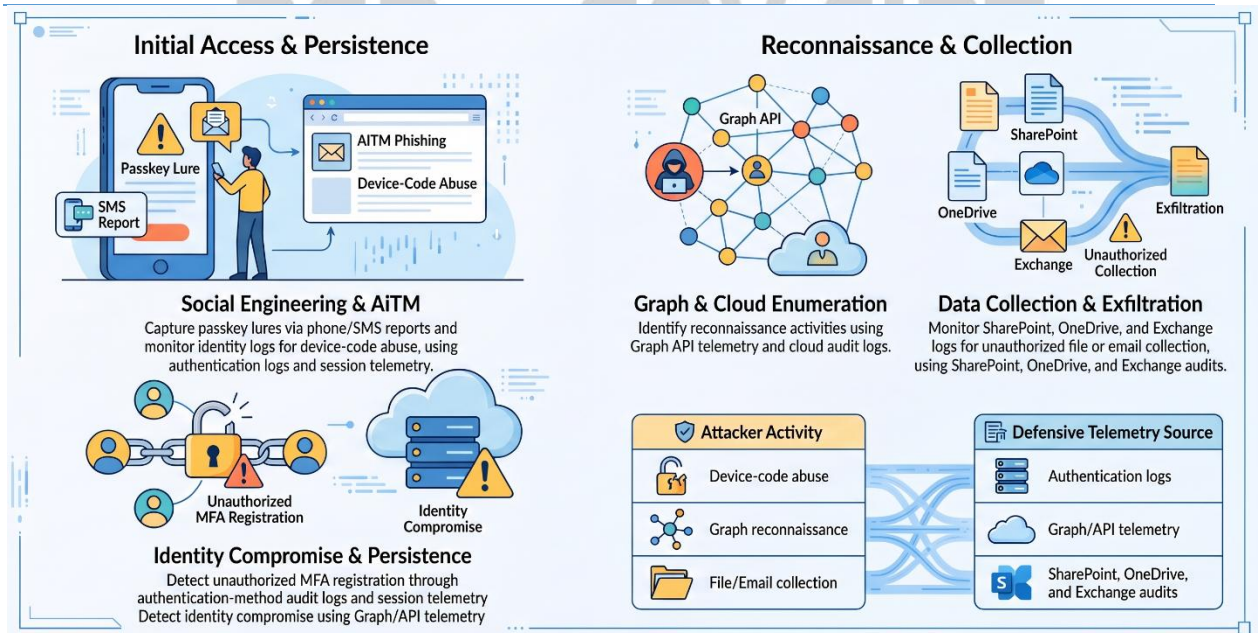

Figure: Detection Opportunities Across the Passkey-Themed Attack Lifecycle

Recommended Actions

Organizations should prioritize the following activities:

- Review recent MFA registrations for unauthorized authentication methods.
- Review newly registered authenticator devices and verify ownership with users.
- Review software-based OTP registrations and identify any unexpected additions.
- Search for unusual device-code authentication activity, particularly where it is inconsistent with established organizational workflows.
- Review sign-ins from unmanaged or previously unseen devices and correlate them with user, location, IP address, and authentication method.
- Correlate anomalous sign-ins with subsequent Microsoft Graph activity, particularly directory, role, application, and authentication-method enumeration.
- Hunt for the reported campaign-associated domains across DNS, proxy, firewall, email-security, and endpoint telemetry.
- Review SharePoint and OneDrive activity for abnormal repository enumeration, file access, synchronization, or download behavior.
- Review Exchange REST/API activity for unusual mailbox, folder, or attachment access.
- Investigate python-httpx user-agent activity when associated with anomalous cloud identities, unusual source infrastructure, or automated data-access patterns. The user-agent should not be treated as a standalone malicious indicator.
- Review access originating from anonymous or residential proxy infrastructure, particularly when combined with unusual authentication or cloud-data access.
- Review recently granted application permissions and OAuth consent, including unexpected enterprise applications, service principals, delegated permissions, or application permissions.

If Compromise Is Confirmed

- For an account confirmed or strongly suspected to be compromised, organizations should immediately:
- Revoke active sessions associated with the affected identity.
- Revoke refresh tokens to invalidate persistent authentication sessions.
- Reset the affected account credentials using the organization's approved identity-recovery procedure.
- Remove all unauthorized MFA/authentication methods registered during or after the suspected compromise.
- Re-register legitimate authentication methods after the account has been secured.
- Review and remove unauthorized OAuth/application grants and investigate newly registered applications or service principals.
- Review mailbox rules and forwarding configurations for unauthorized modifications.
- Determine what cloud data was accessed or downloaded, including SharePoint, OneDrive, Exchange mailboxes, messages, and attachments.
- Identify additional accounts targeted through internal messaging or impersonation, as compromised accounts may have been used to facilitate subsequent social engineering.

References

- https://www.microsoft.com/en-us/security/blog/2026/09/09/passkey-themed-social-engineering-leads-identity-cloud-compromise/
- https://rhisac.org/threat-intelligence/passkey-themed-social-engineering-lures-attempt-to-compromise-identity-and-cloud-platforms/