

# From anonymous user to Global Admin in 45min

... , or not!



**MC2MC**  
—CONNECT—

2Pint



robopack 

wortell

INGRAM<sup>®</sup>  
MICRO



The Collective

 bechtle

 lebon.IT



 VirtualMetric



evri

# ROGIER DIJKMAN

- name: Rogier Dijkman
- located\_in: The Netherlands
- current\_job: Cloud Security Architect
- company: Rubicon Cloud Advisors
- Microsoft MVP (Security / Identity)



MC2MC  
—CONNECT—

# FABIAN BADER



- Lives in Hamburg, Germany
- Cyber Security Architect @ glueckkanja AG
- Microsoft MVP (Security / Azure)
- Organizer of "Purple Elbe Security User Group"

MC2MC  
—CONNECT—

# Agenda

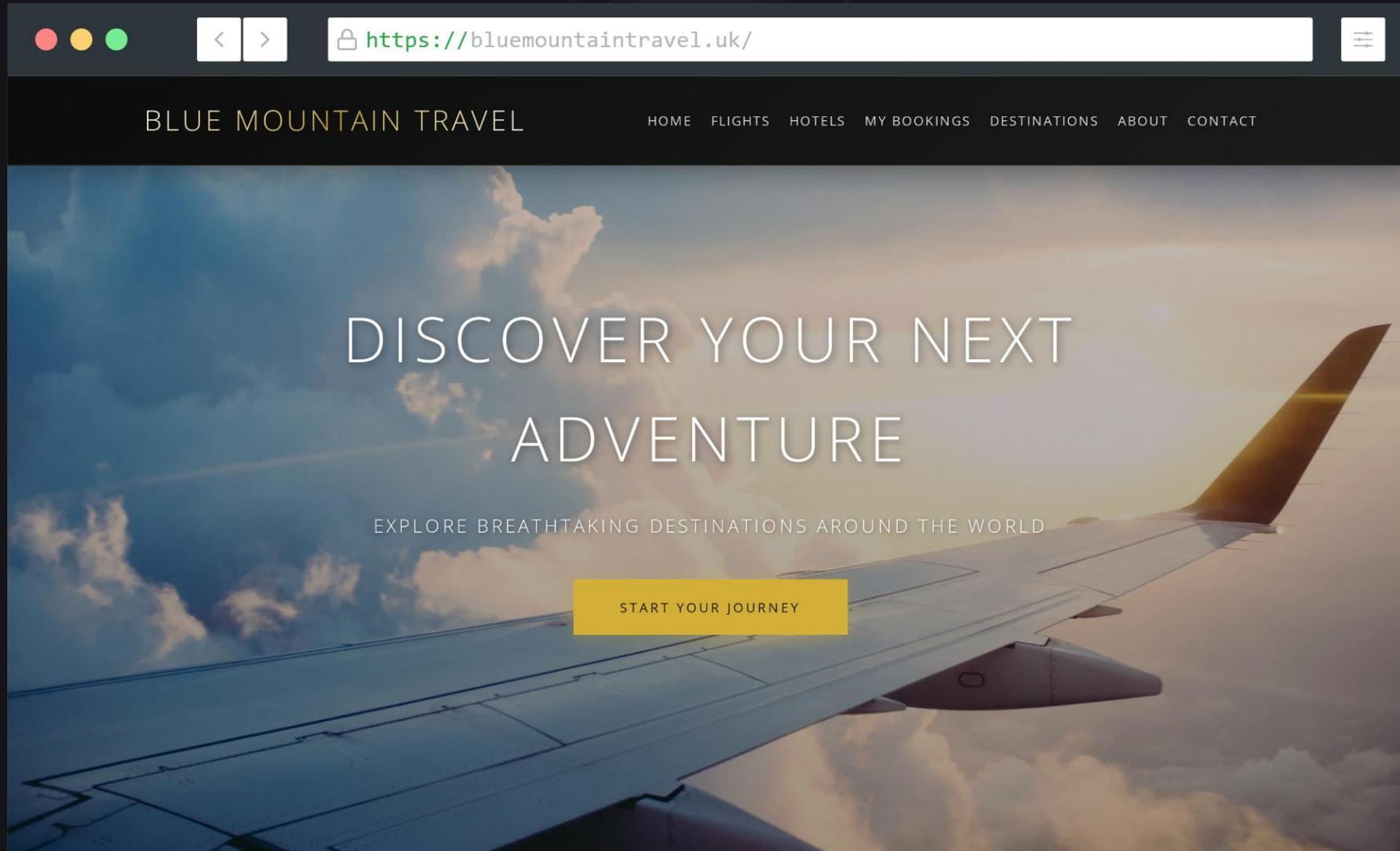
- Meet "Blue Mountain Travel Ltd."
- Live Hacking and Defending
- The end!?

MC2MC  
—CONNECT—

# Blue Mountain Travel

- UK-based travel agency undergoing digital transformation.
- Recently migrated their HR onboarding portal to Azure, using:
  - Azure App Service for the HR portal
  - Azure Files for onboarding document storage
  - Azure SQL for HR database
  - User Assigned Managed Identity (UAMI) for CI/CD automation
  - GitHub Actions for deployment pipelines

# Blue Mountain Travel



BLUE MOUNTAIN TRAVEL

HOME FLIGHTS HOTELS MY BOOKINGS DESTINATIONS ABOUT CONTACT

## DISCOVER YOUR NEXT ADVENTURE

EXPLORE BREATHTAKING DESTINATIONS AROUND THE WORLD

START YOUR JOURNEY

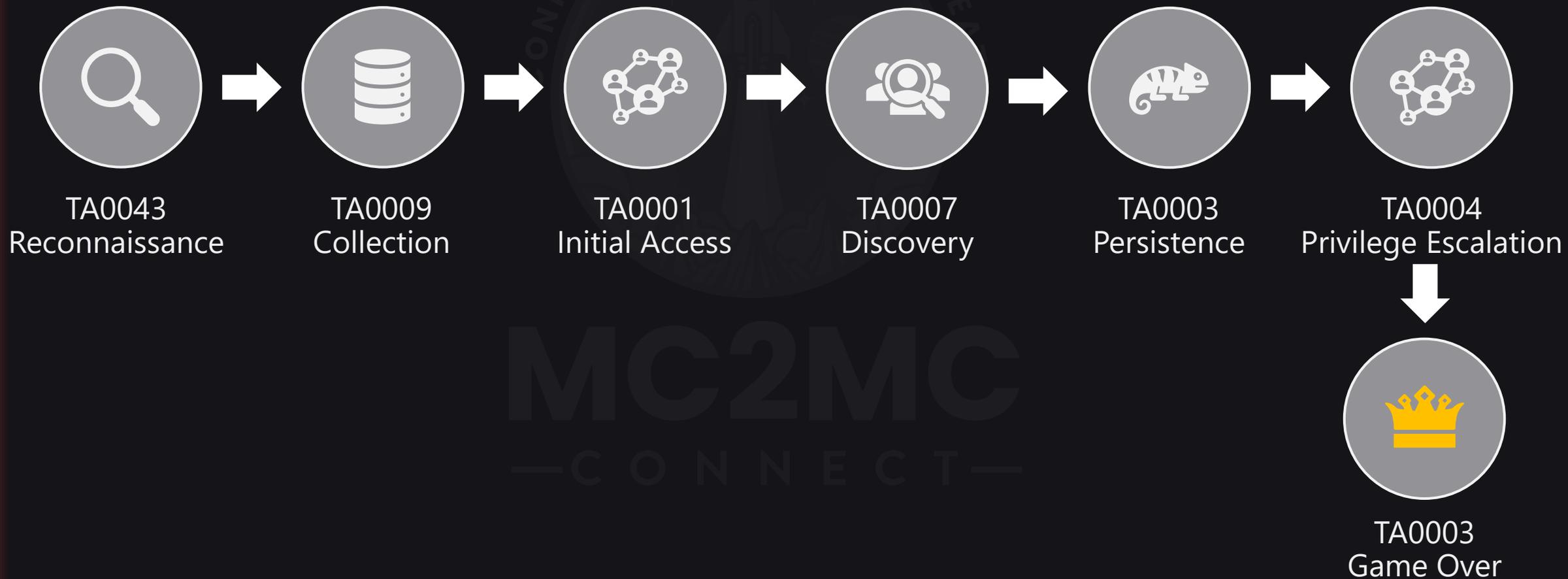
# Protection

- Microsoft Defender XDR + Defender for Cloud
- Microsoft Sentinel
- Additional log sources:
  - Azure Activity
  - Entra ID Sign-in logs
  - Storage Activity Logs
  - User and behaviour analytics

B74CCK@T



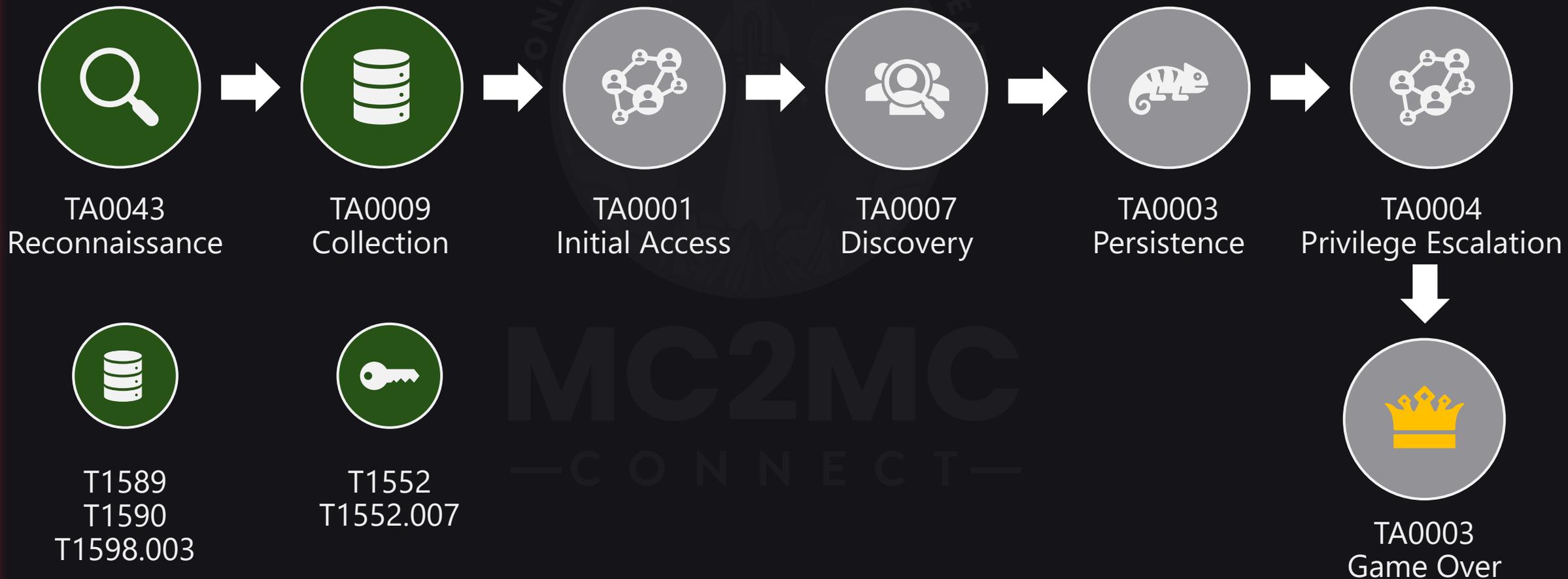
# The attack chain



Phase #1 + #2



# The attack chain



# Detection

- Defender for Cloud - \$10/Storage account/month

## Publicly accessible storage containers have been exposed

Part of incident: Collection incident reported by multiple sources [View incident page](#)

**bluemountainbankdeploy**  
Storage Account

Alert story Maximize

### What happened

Someone scanned the storage account 'bluemountainbankdeploy' and exposed 1 blob containers that allow public access from the internet. This scanning pattern, known as 'blob-hunting', typically indicates an attacker collection tactic in an attempt to find and exfiltrate sensitive data leading to a data breach. A sample of the exposed blob containers: 'templates'. Refer to the General Information and Entities sections for more information.

This alert is triggered by MDC detection  
[View alert page in MDC](#)

### Activities

1/27/2026 10:01:13 AM **Publicly accessible storage containers have been exposed** on a cloud resource

Alert Id	58b7131-7efd-41ee-b977-d9ab79661196
Azure AD user	N/A (Azure AD user authentication was not used)
User agent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.5938.132 Safari/537.36 OPR/102.0.0.0
API type	Blob
Authentication type	Anonymous
Investigation steps	Follow the instructions on how to investigate blob-hunting attempts and what red flags to look for: <a href="https://go.microsoft.com/fwlink/?linkid=2239586">https://go.microsoft.com/fwlink/?linkid=2239586</a> .
Operations types	ListBlobs
Service type	Azure Blobs
Potential causes	Accidental misconfiguration of access levels by someone within the organization, or a threat actor made an unauthorized change in the access

### Publicly accessible storage containers have been exposed

Low | Unknown | New

[Manage alert](#) [Move alert to another incident](#) [Tune alert](#)

#### Details Recommendations

**INSIGHT**

**Quickly classify this alert**

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

[Classify alert](#)

#### Alert state

Classification	Assigned to
Not Set	Unassigned

[Set Classification](#)

#### Alert details

Alert ID	Category
dc2dca1ce5-0a9b-36b0-06a6-4b033ea7c28b	Collection

Detection source	Service source
------------------	----------------

# Detection

- Custom Detections requires Storage Diagnostic Logs

The image shows two screenshots from the Azure portal. The left screenshot displays the 'Diagnostic setting' configuration page for a resource named 'prd'. It includes sections for 'Logs' and 'Metrics'. Under 'Logs', 'audit' and 'allLogs' are selected under 'Category groups', and 'Storage Read', 'Storage Write', and 'Storage Delete' are selected under 'Categories'. Under 'Destination details', 'Send to Log Analytics workspace' is checked, with 'Subscription' set to 'Azure Hacking (MSDN)' and 'Log Analytics workspace' set to 'azh-eus-prd-sentinel ( eastus )'. The 'Metrics' section has 'Transaction' unchecked.

The right screenshot shows an alert titled 'Potential Storage Enumeration or Brute Force Attack' with a severity of 'Medium'. It includes an 'INSIGHT' section with the text 'Quickly classify this alert' and a 'Classify alert' button. Below this, the 'Alert state' is 'Not Set', and the 'Assigned to' field is 'Unassigned'. The 'Alert details' section shows the 'Alert ID' as 'sn3b153f66-b74e-4583-a158-3fccf9a05bb5' and the 'Category' as 'Collection'. The 'Detection source' is 'Scheduled detection' and the 'Service source' is 'Microsoft Sentinel'. The 'Generated on' date is 'Jan 27, 2026 7:16:24 AM'.

# Detection

## Anonymous Retrieval of Azure Blob Versions

Part of incident: Multi-stage incident involving Initial access & Collection involving multiple users reported by multiple sources [View incident page](#)

### What happened

This rule detects a sequence of suspicious activities where an unauthenticated (anonymous) source enumerates the version history of a storage blob and subsequently downloads a blob from the same path within a 10-minute window.

While public access to storage containers may be intentional, attackers frequently target these containers to look for `_soft-deleted_` data or previous versions of files. They do this to uncover sensitive information (such as hardcoded credentials, API keys, or PII) that may have been present in an older version of a file but removed in the current `_live_` version.

ANALYTICS RULE



### Anonymous Retrieval of Azure Blob Versions

■ Low | ● Unknown | ● New

[Manage alert](#) [Move alert to another incident](#)

#### Classification

Not Set

[Set Classification](#)

#### Assigned to

Unassigned

#### Alert details

##### Alert ID

sncf215ade-35ba-4114-a958-a1759c5699dd

##### Category

Collection

# Detection

## Successful Azure Storage File Access from Unauthorized Geo-Location

### What happened

This analytics rule detects successful `_GetFile_` operations performed on Azure Storage accounts from IP addresses located outside of the organization's designated allowed countries (United Kingdom, Netherlands, Germany).

The query analyzes `StorageFileLogs` for successful status codes (200) and resolves the caller's IP address to its geolocation. Access attempts from unexpected countries may indicate compromised credentials, a misconfigured application, or unauthorized data exfiltration attempts.

ANALYTICS RULE



### Successful Azure Storage File Access from Unauthorized Geo-Location

■ Medium | ● Unknown | ● New



Manage alert



Move alert to another incident

#### INSIGHT

#### Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.



**MC2MC**  
—CONNECT—

Demo

# Prevention

- Use Azure Policies to prevent public exposure of storage accounts

The screenshot displays the Microsoft Azure portal interface. At the top, the 'Microsoft Azure' logo is visible on the left, and a search bar on the right contains the text 'Search resources, services, and docs'. Below the navigation bar, the breadcrumb path 'Home > Policy | Definitions >' is shown. The main heading is 'Configure your Storage account public access to be disallowed', with a three-dot menu icon to its right. Underneath the heading, it is identified as a 'Policy definition'. A row of action buttons includes 'Assign policy', 'Edit definition', 'Duplicate definition', 'Select version', and 'Delete definition'. A section titled 'Essentials' with an upward-pointing chevron contains a list of key-value pairs: Name: 'Configure your Storage account public access to be disallowed', Version: '1.0.0', Description: 'Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present securi...', Available Effects: 'Modify', and Category: 'Storage'. At the bottom, there are three tabs: 'Definition' (which is underlined), 'Assignments (0)', and 'Parameters (1)'.

Microsoft Azure

Search resources, services, and docs

Home > Policy | Definitions >

## Configure your Storage account public access to be disallowed

Policy definition

Assign policy Edit definition Duplicate definition Select version Delete definition

### ^ Essentials

Name : Configure your Storage account public access to be disallowed

Version : 1.0.0

Description : Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present securi...

Available Effects : Modify

Category : Storage

Definition Assignments (0) Parameters (1)

# Security recommendations



**bluemountaintravelsa**

Go hunt ...

None

department: Human Resources

purpose: HR Onboarding Documents

sensitivity: Confidential

+1

Overview

Incidents and alerts

**Security recommendations**

Attack paths

Sensitive data

Malware scanning

Export

4 items

Search

Customize columns

Selected filter set: None Save

Risk level: Any



Exposed asset: Any



Asset risk factors: Any



Status: 4 selected



Add filter



Reset all

+5 more

Risk level ⓘ

Recommendation title

Exposed asset

Asset risk factors

Asset attack paths

Recommendation owner

Critical

Storage account public access should be disallowed

bluemountaintravelsa

Exposure to the Internet

0

-

High

Storage accounts should prevent shared key access

Preview

bluemountaintravelsa

Exposure to the Internet

0

-

Low

Storage account should use a private link connection

Preview

bluemountaintravelsa

Exposure to the Internet

0

-

Low

Storage accounts should restrict network access using virtual n...

Preview

bluemountaintravelsa

Exposure to the Internet

0

-

# Secret scanning (not so much)

Cloud Inventory > bluemountaintravelsa



## bluemountaintravelsa

■■■■ None    department: Human Resources    purpose: HR Onboarding Documents    sensitivity: Confidential    tabletop-exercise: vulnerable-deployment

Go hunt    Configure settings    ⋮

Overview    Incidents and alerts    Security recommendations    Attack paths    Sensitive data    Malware scanning

*i* For more information on sensitive data in cloud data resources, [click here.](#) ×

Refresh    Export    0 items    Search    Customize columns

Selected filter set: None ▼    Save

Resource type: Any ×    Sensitivity label: Any ×    Add filter

Name ▼    Resource type ▼    Sensitivity label ▼    Info type ▼    Last scan time ▼

### No sensitive data found

Your resource was scanned, and no sensitive data was discovered

# ID 68: Collection incident

Medium | Active | Unassigned | Unclassified | Last update time: Feb 5, 2026 10:01 AM

- [Attack story](#)
- [Alerts \(3\)](#)
- [Activities \(7\)](#)
- [Assets \(1\)](#)
- [Investigations \(0\)](#)
- [Evidence and Response \(2\)](#)
- [Summary](#)

## Detection & Categories

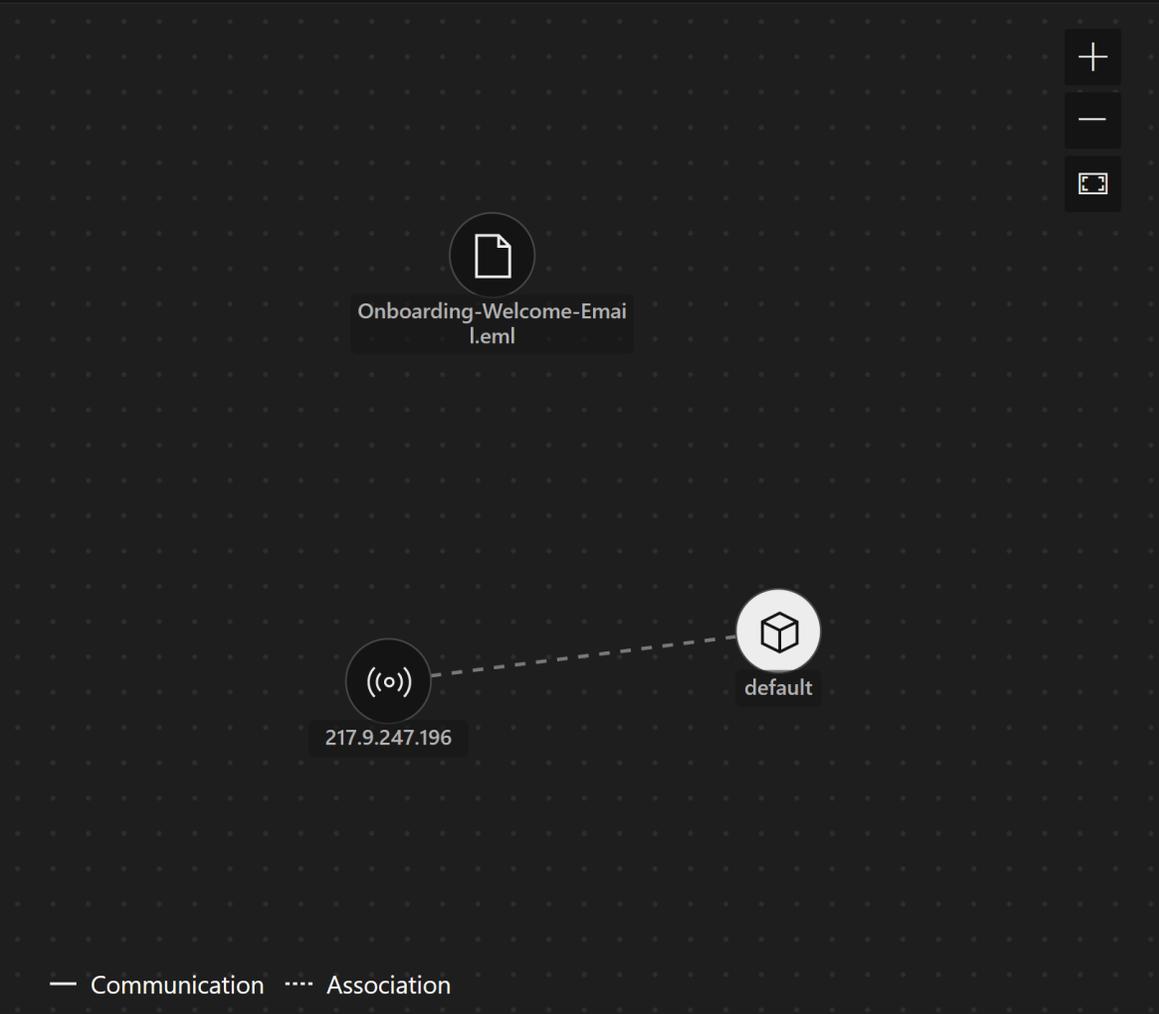
<b>Active alerts</b> 3/3	<b>Categories</b> 1
<b>First activity</b> Feb 5, 2026 9:45:13 AM	<b>Last activity</b> Feb 5, 2026 9:53:45 AM
<b>Creation time</b> Feb 5, 2026 9:56:32 AM	

## Alerts

- Feb 5, 2026 9:45 AM New  
**Potential Storage Enumeration or Brute Force Attack**  
default
- Feb 5, 2026 9:49 AM New  
**Anonymous Retrieval of Azure Blob Versions**
- Feb 5, 2026 9:53 AM New  
**Successful Azure Storage File Access from Unauthorized Geo-Location**

[Report incident inaccuracy](#)

## Incident graph



## Incident details

<b>Priority assessment</b>	Not set
This incident does not yet have a priority assigned.	
<b>Assigned to</b>	Unassigned
<b>Incident ID</b>	68
<b>Classification</b>	Not set
<b>Categories</b>	Collection
<b>First activity</b>	Feb 5, 2026 9:45:13 AM
<b>Creation Time</b>	Feb 5, 2026 9:56:32 AM
<b>Last activity</b>	Feb 5, 2026 9:53:45 AM
<b>Workspaces</b>	azh-eus-prd-sentinel
<b>Incident description</b> ⓘ	
Detected a pattern of failed access attempts against Azure Blob Storage where the failure rate exceeded 90% for a single source IP.	

# Choose your path

App Secret



User  
Password

# Choose your path

App Secret



User  
Password

# Choose *your* path

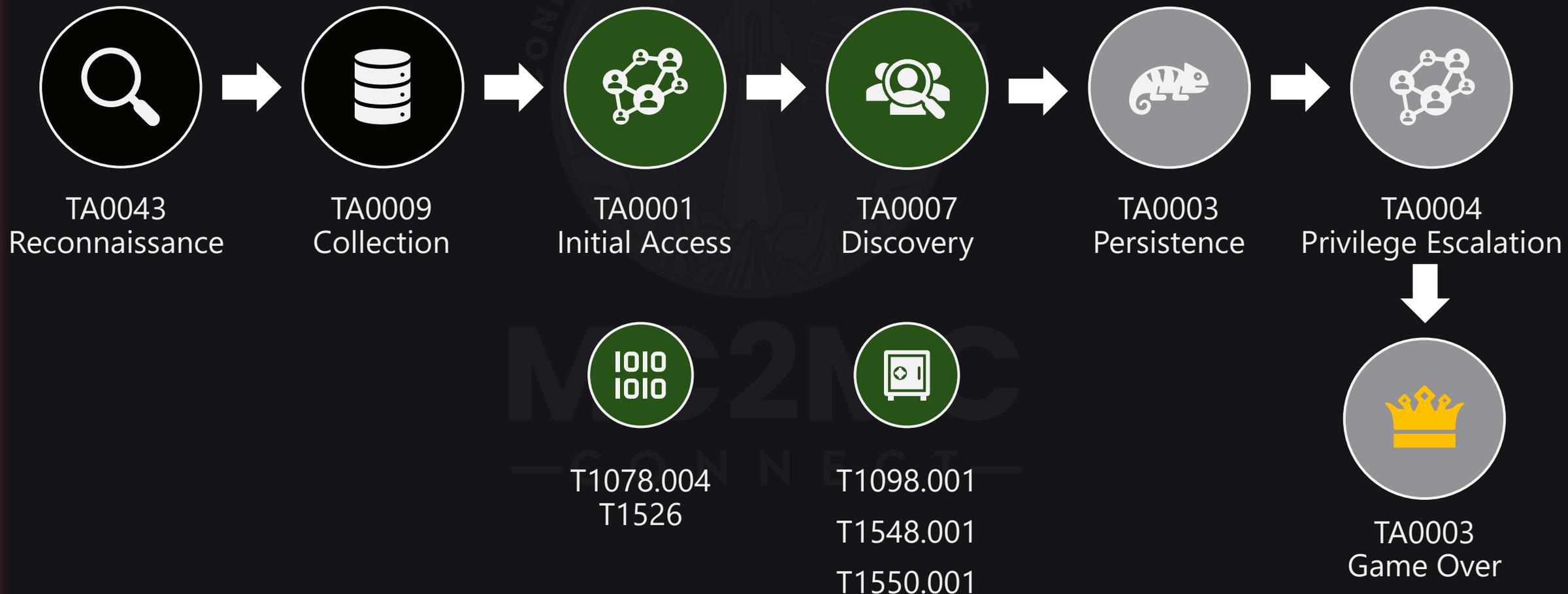
App Secret



Phase #3 + #4



# The attack chain



# AppRoleAssignment.ReadWrite.All

Permission	Justification Given	Actual Need	Real Risk
User.ReadWrite.All	"Create new employee accounts"	Legitimate	Medium
Group.ReadWrite.All	"Add employees to department groups"	Legitimate	Medium
Application.Read.All	"Read app info to validate assignments"	Sounds safe	Low
AppRoleAssignment.ReadWrite.All	"Assign new employees to Salesforce, ServiceNow, etc."	Sounds legitimate	<b>CRITICAL</b>

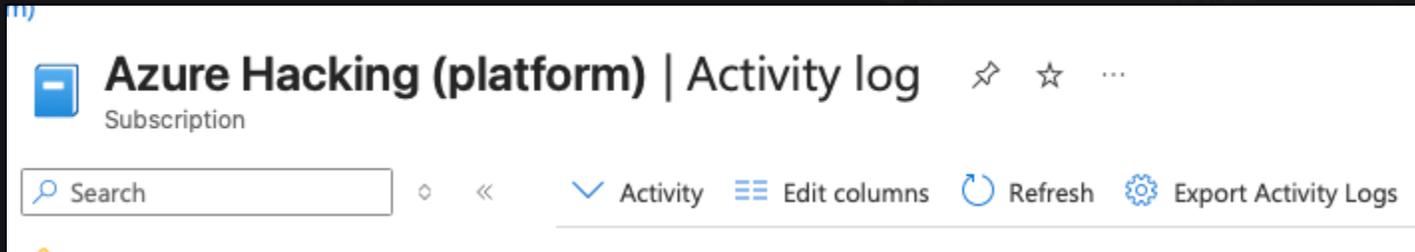
# Detection

- Identity Protection for Workload Identities
- Custom detections
  - Based on location changes
  - Monitor for behavior changes
  - Monitor Microsoft Graph activity for discovery pattern
  - Alert when unknown Federated Identity Providers are used

MC2MC  
—CONNECT—

# Detection

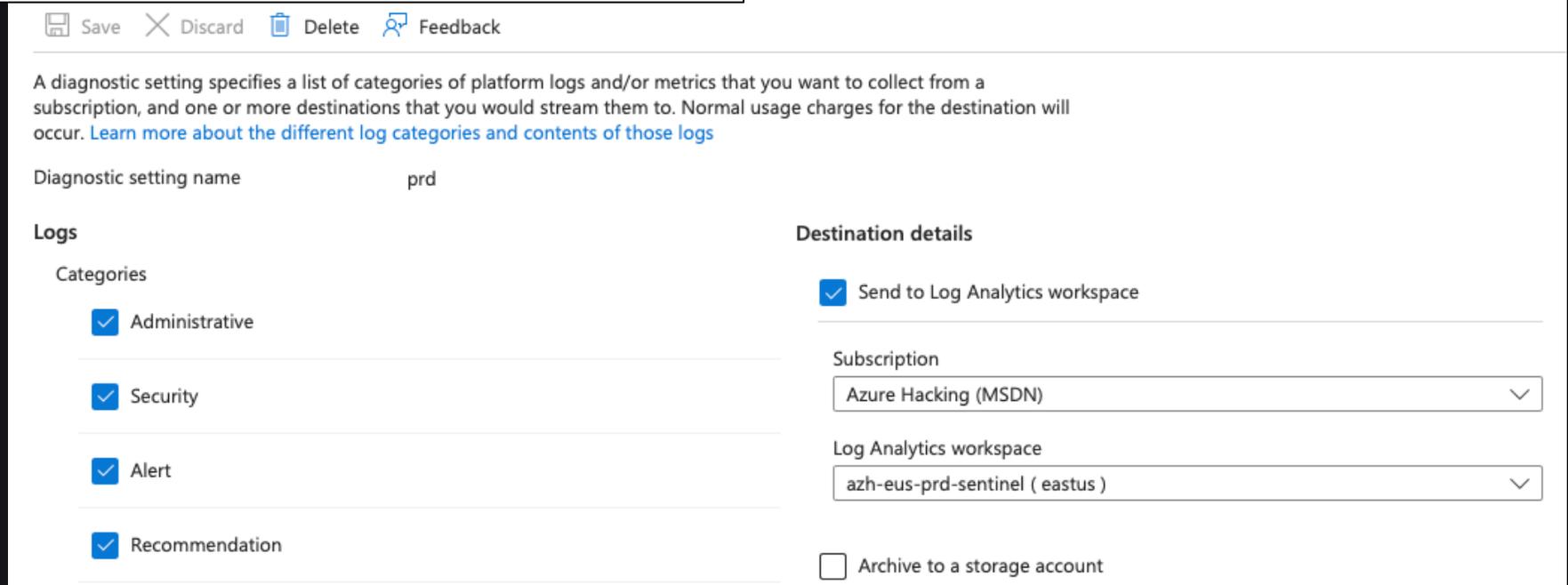
- Custom Detection requires Subscription Diagnostic Logs (free)



Azure Hacking (platform) | Activity log  
Subscription

Search

Activity Edit columns Refresh Export Activity Logs



Save Discard Delete Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a subscription, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name prd

**Logs**

Categories

- Administrative
- Security
- Alert
- Recommendation

**Destination details**

- Send to Log Analytics workspace

Subscription  
Azure Hacking (MSDN)

Log Analytics workspace  
azh-eus-prd-sentinel ( eastus )

Archive to a storage account

# Detection

## Service Principal Sign-in from New Country

Part of incident: Multi-stage incident involving Initial access & Collection involving multiple users reported by multiple sources [View incident page](#)

### What happened

This rule detects successful sign-ins (ResultType == 0) by a Service Principal from a country that has not been observed in the preceding 14 days. It establishes a baseline of `_known_` locations for each AppId over a two-week period and alerts when a login occurs from a location outside of this baseline. This behavior may indicate that a Service Principal's credentials have been compromised and are being used from an anomalous location.

ANALYTICS RULE

### Analytics rule details

Rule name



### Service Principal Sign-in from New Country

Medium | Unknown | New

[Manage alert](#) [Move alert to another incident](#)

INSIGHT

#### Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

# Detection



## Unauthorized Federated Credential Added to Managed Identity

 rogier.dijkman

### What happened

Detected the addition of an unauthorized Federated Identity Credential to a User Assigned Managed Identity.

The activity involved configuring a Managed Identity to trust a specific external repository or organization that was not on the approved allow-list.

This configuration established a potential backdoor, allowing:

- \* Persistence: External workflows (e.g., GitHub Actions) from the unauthorized organization (AttackerOrg) were authorized to exchange their OIDC tokens for valid Azure Access Tokens.
- \* Privilege Escalation: An external actor effectively gained the permissions associated with the internal Managed Identity without requiring a password or secret.
- \* Defense Evasion: The actor utilized legitimate cloud federation protocols to bypass traditional credential monitoring.

ANALYTICS RULE



## Unauthorized Federated Credential Added to Managed Identity

■ Medium | ● Unknown | ● New

 Manage alert  Move alert to another incident

INSIGHT

### Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

### Alert state

Classification

Not Set

[Set Classification](#)

Assigned to

Unassigned

# Detection

## Service Principal Enumeration of App Role Assignments

Part of incident: Multi-stage incident involving Initial access & Collection involving multiple users reported by multiple sources [View incident page](#)

### What happened

This rule detects a non-human identity (Service Principal or Managed Identity) utilizing the Microsoft Graph API to list App Role assignments (`/appRoleAssignments`). The query filters for `_GET_` requests where the `_UserId_` is empty, isolating activity performed by applications rather than interactive users.

This behavior is potentially suspicious as it is a common reconnaissance technique. An attacker who has compromised a Service Principal may use this API call to map out privileges and discover high-value permissions (e.g., `_Directory.ReadWrite.All_` or `_RoleManagement.ReadWrite.Directory_`) assigned to that principal or others, facilitating lateral movement or privilege escalation.

ANALYTICS RULE



### Service Principal Enumeration of App Role Assignments

Medium | Unknown | New

[Manage alert](#) [Move alert to another incident](#)

INSIGHT

#### Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

# Detection

ST. COLLABORATE

## Known Attack Tool Execution: BlackCat Enumeration

 rogier.dijkman

### What happened

Detected a sequence of Microsoft Graph API requests matching the behavioral signature of the \_BlackCat\_ Azure post-exploitation tool.

The source entity executed a batch of high-volume queries targeting specific directory objects that are highly indicative of malicious reconnaissance. The activity exceeded a 70% match rate against the tool's known fingerprint.

This activity indicated an attacker had already authenticated and was attempting to:

- \* Enumerate Permissions: Probing for Service Principal role assignments and OAuth2 permission grants to identify privilege escalation paths.
- \* Map High-Value Targets: Identifying transitiveMemberOf relationships to locate administrative accounts and sensitive directory roles.
- \* Batch Discovery: utilizing the \$batch endpoint to evade rate limits while rapidly mapping the environment.

Custom detection



## Known Attack Tool Execution: BlackCat Enumeration

■ ■ ■ Medium | ● Unknown | ● New

 Manage alert  Move alert to another incident

INSIGHT

### Quickly classify this and 1 similar alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

[View 1 similar alert](#) ⓘ

### Alert state

Classification

Not Set

[Set Classification](#)

Assigned to

Unassigned

# Prevention

- Use Conditional Access for workload identities
- Limit to known IP ranges if possible
- Do not use secrets but certificates or federated identities

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name \*  
Block High Risk SPs ✓

Assignments  
Users, agents or workload identities ⓘ  
All owned service principals

Target resources ⓘ  
No target resources selected

Network **NEW** ⓘ  
Not configured

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
Block access

Session ⓘ

Control access based on who the policy will apply to, such as users and groups, agents, workload identities, directory roles, or external guests. [Learn more](#)

What does this policy apply to?  
Workload identities

**Include** Exclude

None  
 All owned service principals  
 Select service principals

**i** Policy only applies to single tenant service principals owned by your organization. [Learn more](#)

Name \*  
Block if outside of trusted network ✓

Assignments  
Users, agents or workload identities ⓘ  
Specific service principals included

Target resources ⓘ  
No target resources selected

Network **NEW** ⓘ  
Any network or location and all trusted locations excluded

Conditions ⓘ  
1 condition selected

Access controls

Grant ⓘ  
Block access

Session ⓘ  
0 controls selected

What does this policy apply to?  
Workload identities

**Include** Exclude

None  
 All owned service principals  
 Select service principals

Select service principals based on attributes ⓘ  
None

Select  
1 service principal selected

**i** Policy only applies to single tenant service principals owned by your organization. [Learn more](#)

Application #1  
565c3eb0-2dd5-4601-bab1-28c43b5ed...

# Prevention

- Azure Policy: Limit Federated Credentials to allowed issuers

**[Preview]: Managed Identity Federated Credentials should be from allowed issuer types** ...

Policy definition

Assign policy Edit definition Duplicate definition Select version Delete definition

^ Essentials

Name	: [Preview]: Managed Identity Federated Credentials should be from allowed issuer types	Definition location	: --
Version	: 1.0.0-preview	Definition ID	: /providers/Microsoft.Authorization/policyDefinitions/2571b7c3-3056-4a61-b00a-9bc5232234f5
Description	: This policy limits whether Managed Identities can use federated credentials, which common issuer types are allowed, and provides a list of allowed is...	Type	: Built-in
Available Effects	: Audit	Mode	: All
Category	: Managed Identity		

Definition Assignments (0) Parameters (7)

Name	Allow Federated Credentials
Type	Boolean
Default Value	false
Name	Allow AKS
Type	Boolean
Default Value	false
Name	Allow GitHub
Type	Boolean
Default Value	false
Name	Allow AWS
Type	Boolean
Default Value	false
Name	Allow GCS
Type	Boolean
Default Value	false
Name	Allowed Exception Issuers
Type	Array
Default Value	[]

# Prevention

- Azure Policy: Limit Federated Credentials to trusted repository owners

## [Preview]: Managed Identity Federated Credentials from GitHub should be from trusted repository owners

Policy definition

 Assign policy  Edit definition  Duplicate definition  Select version  Delete definition

### ^ Essentials

Name : [Preview]: Managed Identity Federated Credentials from GitHub should be from trusted repository owners  
Version : 1.0.1-preview  
Description : This policy limits federation with GitHub repos to only approved repository owners.  
Available Effects : Audit  
Category : Managed Identity

Definition    Assignments (0)    Parameters (3)

Name            Allowed Repo Owners  
Type            Array

Name            Allowed Repo Exception  
Type            Array  
Default Value    []

# Prevention

## Password addition restriction ...

 Refresh |  Got feedback?

Status  Off

Policy name

Policy description

[Block password addition](#)

[Restrict max password lifetime](#)

[Block custom passwords](#)

Certificate restrictions

[Restrict max certificate lifetime](#)

Identifier URI restrictions

## Restrict password lifetime ...

 Refresh |  Got feedback?

Status

Policy name

Policy description

## Block custom passwords ...

 Refresh |  Got feedback?

Status  Off

Policy name Block custom passwords

Policy description Policy blocking the addition of custom passwords, meaning new passwords that are added must be system-generated

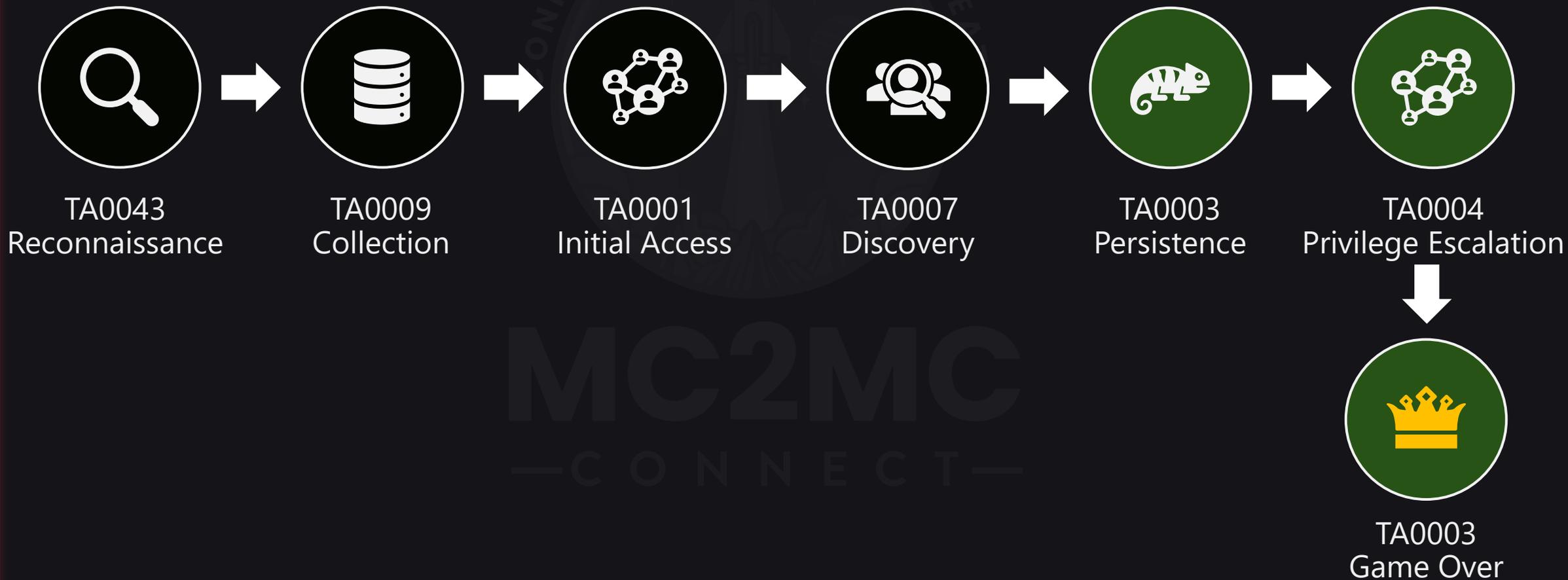
Phase #5



# Phase #5



# The attack chain



# Detection

- Custom detections
  - Assignment of high privileged roles to non-human identities
  - Assignment of high privileged roles outside of PIM
  - Assignment of high privileged roles to non control plane admin
- Microsoft email

 Azure Active Directory is now Microsoft Entra ID. [Learn More.](#)

## The Global Administrator role for the Azure Hacking (ID: 3da86d62-c862-48da-973f-487ab98166a8) directory was assigned outside of PIM

Always use Microsoft Entra ID (ME-ID) Privileged Identity Management (PIM) to manage your privileged directory roles.

### Assignment details:

Settings	Value
User:	Azure-Backup-Automation-Service
Role:	Global Administrator
Assigner:	
Detected on:	January 27, 2026 21:54 UTC

[View assignment >](#)

[Learn more about Microsoft Entra Privileged Identity Management >](#)

# Detect

- Custom de
- Assignme
- Assignme
- Assignme
- Microsoft e

ies

admin

# Detection

## Service Principal Added to Global Administrator Role

User

### What happened

This rule detects when a Service Principal is granted the Global Administrator role in Entra ID (formerly Azure AD). Assigning highly privileged roles to non-human accounts (Service Principals) increases the attack surface and is often an indicator of persistence mechanisms or privilege escalation by an attacker.

Note: The query filters for a specific Role Object ID (39a06fbc...). Ensure this ID matches the Global Administrator Role Object ID in your specific tenant, or replace it with the standard Global Admin Role Template ID (62e90394-69f5-4237-9190-012177145e10) for broader applicability.

ANALYTICS RULE



### Service Principal Added to Global Administrator Role

High | Unknown | New

Manage alert | Move alert to another incident

INSIGHT

#### Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

# Detection

## Privileged Role Assignment Outside of PIM

2 Users

### What happened

Detected that a user account was assigned to an Azure AD directory role without using Privileged Identity Management (PIM). This activity indicated that standard security governance controls—such as Just-In-Time (JIT) access, approval workflows, and time-bound duration—were bypassed. This action created `_standing access_` (permanent privileges) for the target account, which is a significant security risk indicating:

- \* Persistence: An attacker solidifying their foothold by hard-coding an account into a high-privileged role to survive future token resets or PIM policy changes.
- \* Policy Violation/Evasion: An administrator intentionally circumventing audit trails and justification requirements associated with PIM.

ANALYTICS RULE



### Privileged Role Assignment Outside of PIM

High | Unknown | New



Manage alert



Move alert to another incident

INSIGHT

#### Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification

Assigned to

# Unified XDR = Unified Incident

## ID 28: Multi-stage incident involving Initial access & Collection involving ...

Manage incident Tasks

High Active Unassigned Unclassified Last update time: Feb 3, 2026 3:14 PM

Attack story Alerts (33) Activities (80) Assets (8) Investigations (0) Evidence and Response (6) Summary

### Detection & Categories

Active alerts: 33/33 Categories: 5

First activity: Feb 2, 2026 2:55:13 PM Last activity: Feb 3, 2026 2:43:29 PM

Creation time: Feb 2, 2026 3:06:21 PM

### Alerts

- Feb 2, 2026 2:55 PM New Potential Storage Enumeration or Brute Force Attack default
- Feb 2, 2026 3:00 PM New Anonymous Retrieval of Azure Blob Versions
- Feb 2, 2026 5:10 PM New Potential Storage Enumeration or Brute Force Attack default
- Feb 2, 2026 5:16 PM New

Report incident inaccuracy

### Incident graph

Layout Group similar nodes

```
graph TD; A[Onboarding-Welcome-Email] --- B[Azure-Backup-Automation-Service]; B --- C[2 Users]; C --- D[2 IPs]; D --- E[github-backup-automation]; E --- F[2 IPs];
```

Communication Association

### Priority assessment

100

This incident is ranked as top priority and requires immediate attention.

Notable priority factors:

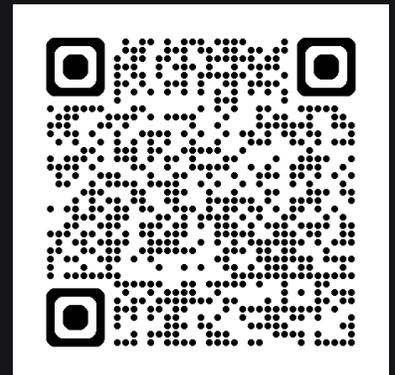
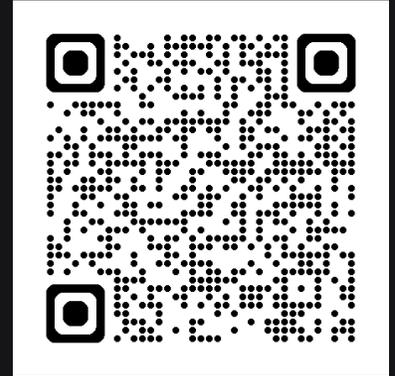
- 5 Notable alert types: Service Principal Enumeration of App Role Assignments, Anonymous Retrieval of Azure Blob Versions, Privileged Role Assignment Outside of PIM, Known Attack Tool Execution: BlackCat Enumeration, Potential Storage Enumeration or Brute Force Attack
- 3 Notable MITRE tactics and techniques: Cloud Groups (T1069.003), Cloud Storage Object Discovery (T1619), Additional Cloud Roles (T1098.003)

### Incident details

Assigned to	Incident ID
Unassigned	28
Classification	Categories
Not set	Initial access

# Tools

- Blackcat
  - <https://github.com/azurekid/blackcat>
- maester
  - <https://maester.dev/>
  - Fully automated and free best practice analysis
  - 100s of tests from the community for the everybody
- Detections
  - <https://github.com/f-bader/AzSentinelQueries/tree/master/AnalyticsRules>



# Thank you



Please give feedback