Abusing Teams privacy, security, and compliance



Dr. Nestori Syynimaa (@DrAzureAD)
Senior Principal Security Researcher at Secureworks
MVP, MVSR





Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks
 CTU
- Creator of AADInternals toolkit
- MVP & MS Most Valuable Security Researcher 2021

Contact details

- nsyynimaa@secureworks.com
- Twitter: <u>@DrAzureAD</u>
- https://linkedin.com/in/nestori
- https://o365blog.com













Contents

- Extracting Teams content as a guest user
- Bypassing Teams policies
- Bypassing MCAS Teams policies







AADInternals

- PowerShell module (script)
- Azure AD & Microsoft 365 administration and hacking toolkit
- Open source:
 - https://github.com/gerenios/aadinternals
 - https://o365blog.com/aadinternals/
- Easy to install and use:

```
C:\PS> Install-Module AADInternals
C:\PS> Import-Module AADInternals
```







Extracting Azure AD content as a guest user









/_				
	Recon	Compromise	Persistence	Actions on Intent
Outsider	Get-AADIntTenantDomains Get-AADIntOpenIDConfiguration Get-AADIntLoginInformation	Invoke-AADIntPhishing		
Get-AADIntAzureInformation Get-AADIntSPOSiteUsers Get-AADIntSPOSiteGroups Invoke-AADIntReconAsGuest Invoke-AADIntUserEnumerationAsGuest				
				New-AADIntBulkPRTToken Join-AADIntDeviceToAzureAD Join-AADIntDeviceToIntune
Admin	Invoke-AADIntUserEnumerationAsInsider Get-AADIntAzureSubscriptions	Grant-AADIntAzureUserAccessAdminRole Set-AADIntAzureRoleAssignment Invoke-AADIntAzureVMScript Register-AADIntPTAAgent Set-UserMFA Set-UserMFAApps	ConvertTo-AADIntBackdoor Set-AADIntPassThroughAuthentication	New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal
On-prem admin		Export-AADIntADFSSigningCertificate Get-AADIntSyncCredentials Set-AADIntUserPassword Install-AADIntPTASpy		New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal
https://o365blog.com/aadkillchain				

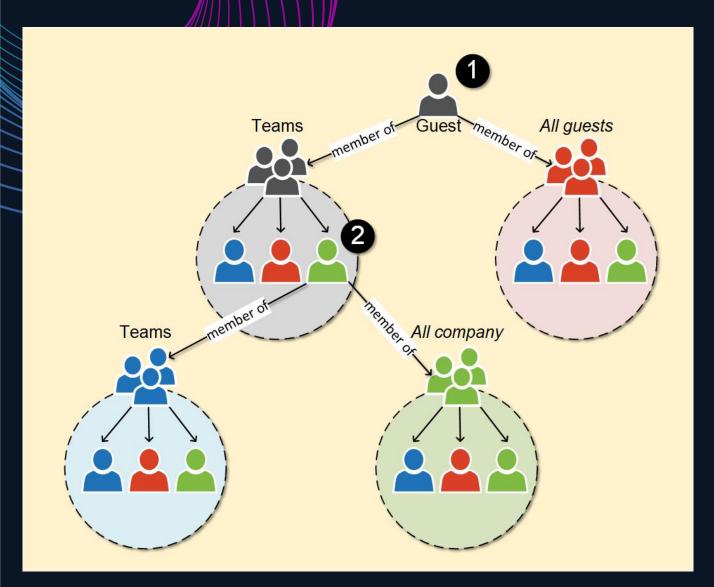
Guest user permissions

- Guest users *
 - Can't browse information from the tenant
 - Can retrieve information about others by providing UPN or GUID
 - Can read properties of groups they belong to
 - Can't view information about any other tenant objects





User enumeration



 Azure AD traversal possible if any "starting point" is known!



DEMO!



Blogged on August 7th 2020

Quest for guest access: Azure Active Directory reconnaissance as a guest







External collaboration settings				
☐ Save X Discard				
Guest user access				
Guest user access restrictions (Preview) ①				
Learn more Guest users have the same access as members (most inclusive)				
Guest users have limited access to properties and memberships of directory objects				
Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)				



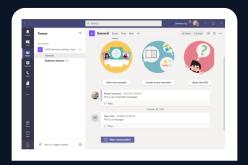
Bypassing Teams Security Policies







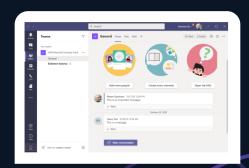
During the Teams start-up

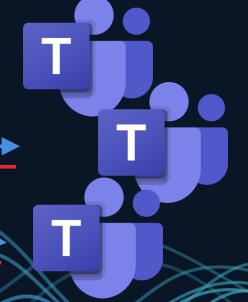


https://teams.microsoft.com/api/mt/../useraggregatesettings

messagingPolicy, meetingPolicy, applicationPolicy









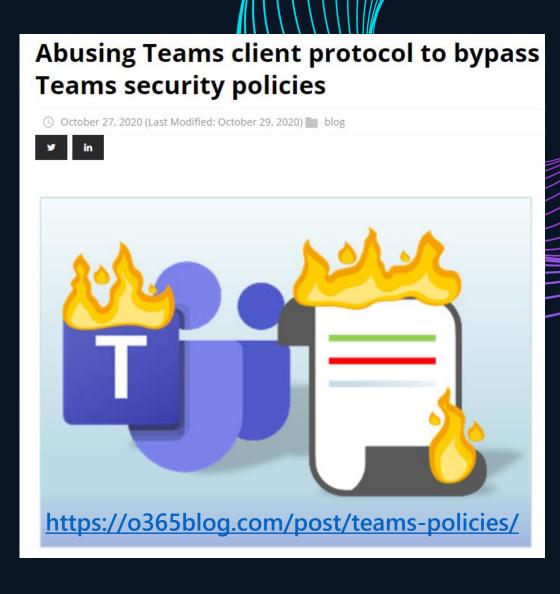
Example: messagingPolicy

Bypassing Teams Policies

```
messagingPolicy": {
          "value":
             "allowUserEditMessage": false,
              "allowUserDeleteMessage": false,
              "allowUserChat": false,
              "allowGiphy": true,
 6
              "giphyRatingType": "Moderate",
              "allowGiphyDisplay": true,
 8
 9
              "allowPasteInternetImage": true,
10
              "allowMemes": true,
11
              "allowStickers": true,
              "allowUserTranslation": true,
12
              "allowUrlPreviews": true.
13
              "readReceiptsEnabledType": "UserPreference",
14
15
              "allowImmersiveReader": true,
16
              "allowPriorityMessages": true,
              "audioMessageEnabledType": "ChatsAndChannels",
17
              "channelsInChatListEnabledType": "DisabledUserOverride",
18
19
              "allowRemoveUser": true,
              "allowSmartReply": true
20
21
22
```

About client-side "security"

- CWE-602: <u>Client-Side</u> <u>Enforcement of Server-Side Security</u>
 - "The software is composed of a server that relies on the client to implement a mechanism that is intended to protect the server."
 - ".. an attacker can modify the client-side behavior to bypass the protection mechanisms.."







Accessing Teams via API

- Option 1: MS Graph API
 - Security enforced on the server-side (3)
 - Create & manage Teams and channels
 - Chat (send messages)
- Option 2: Teams internal API
 - Client-side security
 - Create & manage Teams and channels
 - Chat (send, edit, and remove messages)







DEMO!



Summary

- Guest users can extract data from Teams
 - To mitigate, restrict guest users' rights to a minimum!
- Teams client is responsible for applying security settings & policies
 - Deletion seem to be enforced in the cloud 🖾 🖾
- Some Teams security settings can be bypassed with direct Teams API calls
 - Teams security settings are NOT a security measure!
 - MS Cloud App Security (MCAS) is NOT a security measure!







Thank you!

Questions..?





