

# Abusing Teams privacy, security, and compliance

Dr. N Syynimaa | Secureworks | MVP



Sponsored by



Microsoft Teams



Microsoft Tech Community

# Who?

- Dr. Nestori Syynimaa
- Senior Principal Security Researcher @ Secureworks CTU
- Creator of AADInternals toolkit

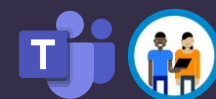
## Contact details

- [nsyynimaa@secureworks.com](mailto:nsyynimaa@secureworks.com)
- Twitter: [@DrAzureAD](https://twitter.com/DrAzureAD)
- <https://linkedin.com/in/nestori>
- <https://o365blog.com>



# Contents

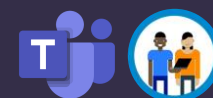
- Extracting Teams content as a guest user
- Bypassing Teams policies



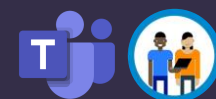
# AADInternals

- 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 Teams content as a guest user





# Azure AD and Microsoft 365 kill chain

	Recon	Compromise	Persistence	Actions on Intent
<b>Outsider</b>	Get-AADIntTenantDomains Get-AADIntOpenIDConfiguration Get-AADIntLoginInformation	Invoke-AADIntPhishing		
<div style="border: 1px solid black; padding: 5px;"> <p>Get-AADIntAzureTenants Get-AADIntAzureInformation Get-AADIntSPOSiteUsers Get-AADIntSPOSiteGroups <b>Invoke-AADIntReconAsGuest</b> <b>Invoke-AADIntUserEnumerationAsGuest</b></p> </div>				
	Invoke-AADIntReconAsInsider Invoke-AADIntUserEnumerationAsInsider			New-AADIntBulkPRTToken Join-AADIntDeviceToAzureAD Join-AADIntDeviceToIntune
<b>Admin</b>	Get-AADIntAzureSubscriptions	Grant-AADIntAzureUserAccessAdminRole Set-AADIntAzureRoleAssignment Invoke-AADIntAzureVMScript Register-AADIntPTAAgent Set-UserMFA Set-UserMFAApps	ConvertTo-AADIntBackdoor Set-AADIntPassThroughAuthentication	New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal
<b>On-prem admin</b>		Export-AADIntADFSSigningCertificate Get-AADIntSyncCredentials Set-AADIntUserPassword Install-AADIntPTASpy		New-AADIntSAMLToken New-AADIntKerberosTicket Open-AADIntOffice365Portal

<https://o365blog.com/aadkillchain/>

# Guest user permissions

Extracting Teams content as a guest user

## Guest users \*

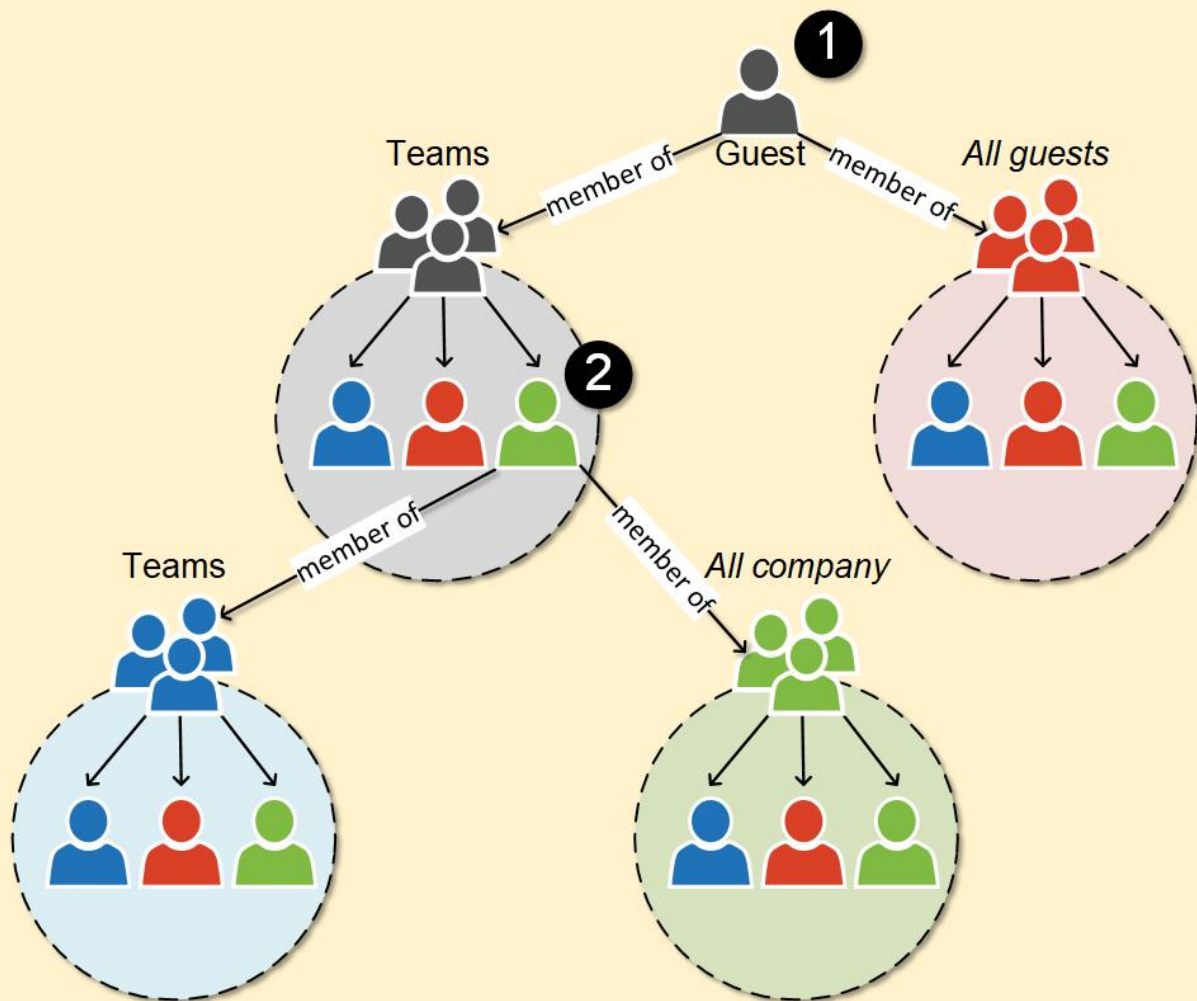
- Can't browse information from the tenant
- Can retrieve information about others by providing UPN or GUID
- Can read properties of groups they belong to
- Can't view information about any other tenant objects

\*) <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions>



# User enumeration

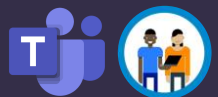
Extracting Teams content as a guest user



- Azure AD traversal possible if any “starting point” is known!



# DEMO!

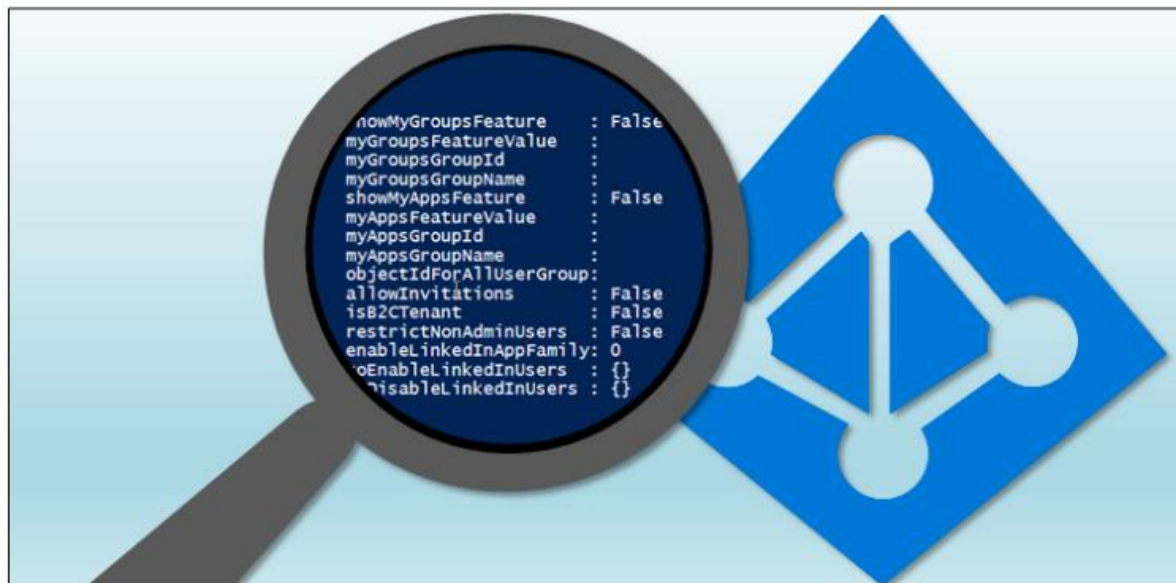


# Blogged on August 7<sup>th</sup> 2020

Extracting Teams content as a guest user

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

🕒 June 14, 2020 (Last Modified: September 06, 2020) 📁 blog



```
showMyGroupsFeature : False
myGroupsFeatureValue :
myGroupsGroupId :
myGroupsGroupName :
showMyAppsFeature : False
myAppsFeatureValue :
myAppsGroupId :
myAppsGroupName :
objectIdForAllUserGroup :
allowInvitations : False
isB2CTenant : False
restrictNonAdminUsers : False
enableLinkedInAppFamily : 0
enableLinkedInUsers : {}
disableLinkedInUsers : {}
```

**TunaMania** @tuna\_gezer · Aug 8  
Great post Nestori, as always! Current guest permissions are around limiting enumerate, anyone who doesn't read the doc miss this detail! We are working on a new feature which will address a large set of your points in the blog, you might need to update the post very soon 😊

1 3

**Dr. Nestori Syynimaa** @NestoriSyynimaa · Aug 8  
Looking forward to that!

2 1

### External collaboration settings

📁 Save ✕ Discard

#### Guest user access

Guest user access restrictions (Preview) ⓘ

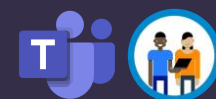
[Learn more](#)

- 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)

<https://o365blog.com/post/quest-for-guest/>

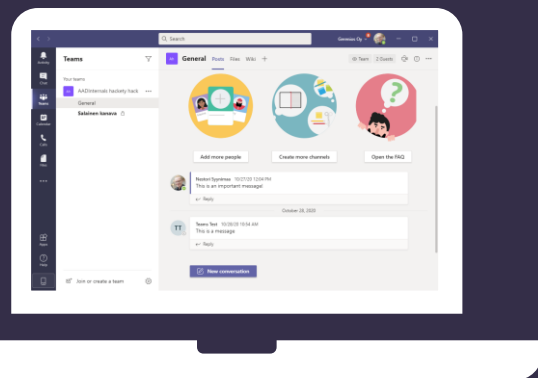


# Bypassing Teams Security Policies



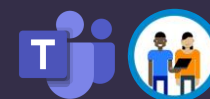
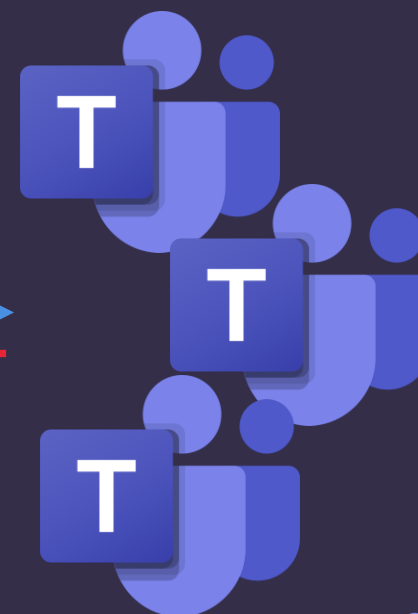
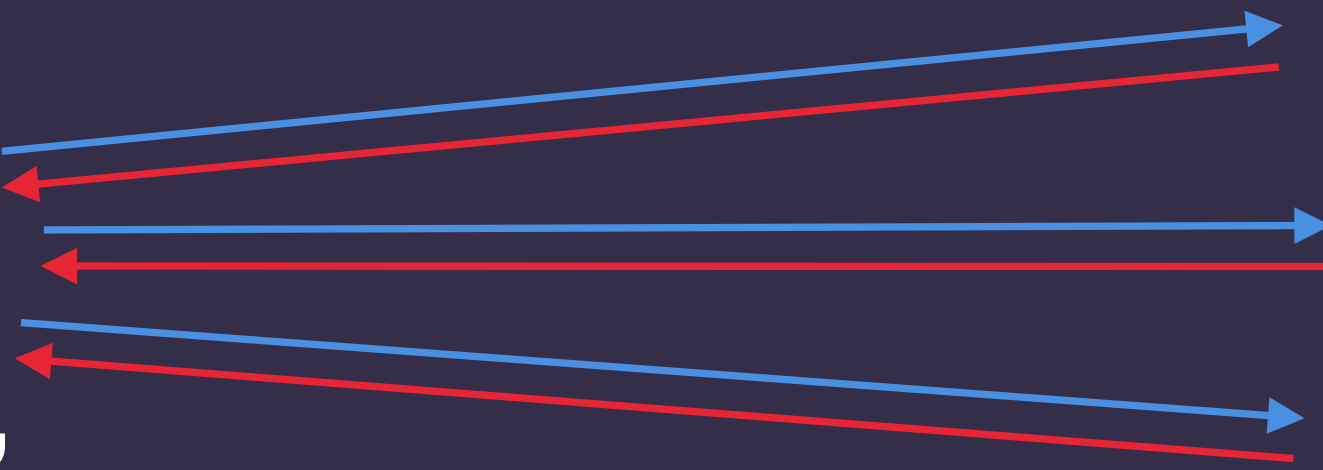
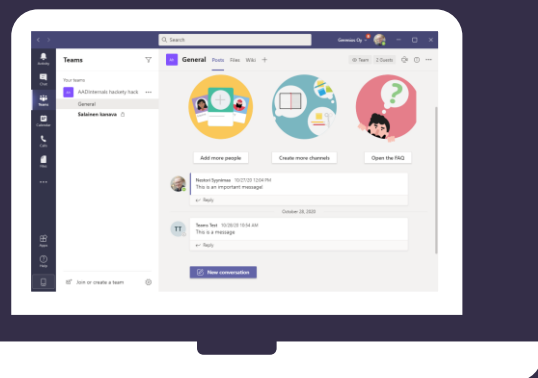
# During the Teams start-up

## Bypassing Teams Policies



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

messagingPolicy, meetingPolicy, applicationPolicy



# Example: messagingPolicy

## Bypassing Teams Policies

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

# About client-side "security"

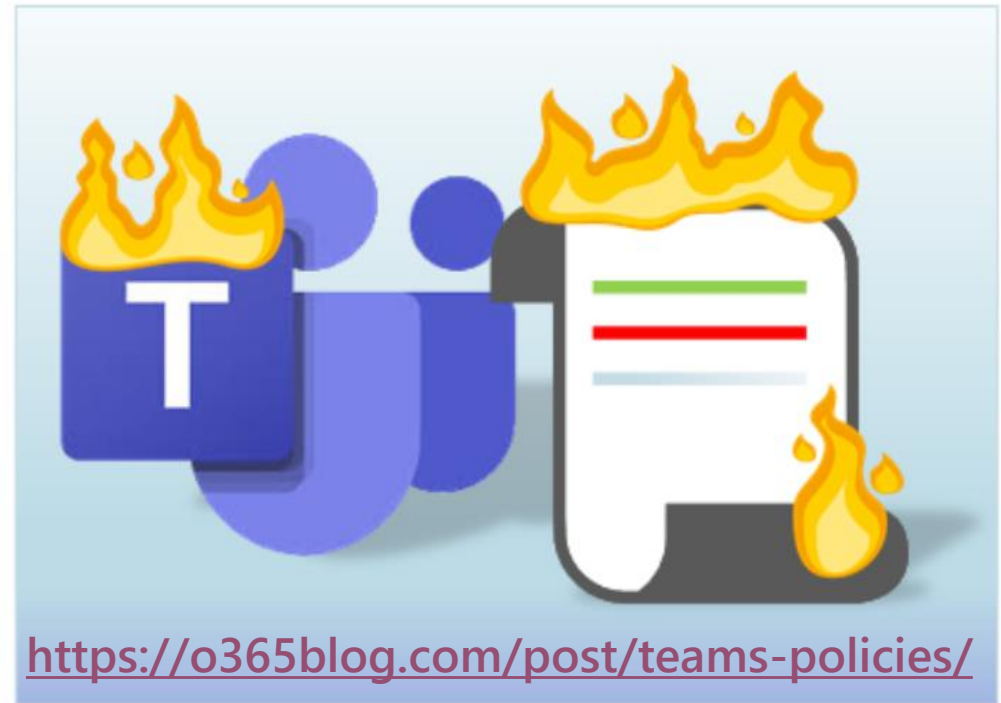
Bypassing Teams Policies

## CWE-602: Client-Side Enforcement of Server-Side Security

- *"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.."*

## Abusing Teams client protocol to bypass Teams security policies

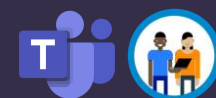
🕒 October 27, 2020 (Last Modified: October 29, 2020) 📄 blog



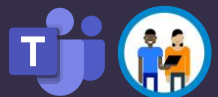
# Accessing Teams via API

Bypassing Teams Policies

- **Option 1: MS Graph API**
  - Security enforced on the server-side 😊
  - 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)



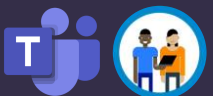
# DEMO!





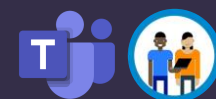
# Summary

- Guest users can extract data from Teams
  - To mitigate, restrict guest users' rights to a minimum!
- Teams security settings can be bypassed with direct Teams API calls
  - Teams security settings are **NOT** a security measure!



Thank you!

Questions..?



# Rate my session & Calls to Action



Rate this session



Attend more sessions and join our keynotes at 19.00 CET



Show your love for Teams Nation on Twitter and LinkedIn using #TeamsNation and @TeamsNation

<https://teamsnation.rocks/feedback>