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
- Twitter: @DrAzureAD
- https://linkedin.com/in/nestori
- https://o365blog.com

Contents

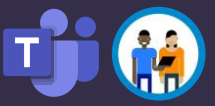
- Extracting Teams content as a guest user
- Bypassing Teams policies

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
Outsider	Get-AADIntTenantDomains Get-AADIntOpenIDConfiguration Get-AADIntLoginInformation	Invoke-AADIntPhishing		
	Get-AADIntAzureTenants Get-AADIntAzureInformation Get-AADIntSPOSiteUsers Get-AADIntSPOSiteGroups Invoke-AADIntReconAsGuest Invoke-AADIntUserEnumerationAsGuest			
	Invoke-AADIntReconAsInsider Invoke-AADIntUserEnumerationAsInsider			New-AADIntBulkPRTToken Join-AADIntDeviceToAzureAD Join-AADIntDeviceToIntune
Admin	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

Extracting Teams content as a guest user

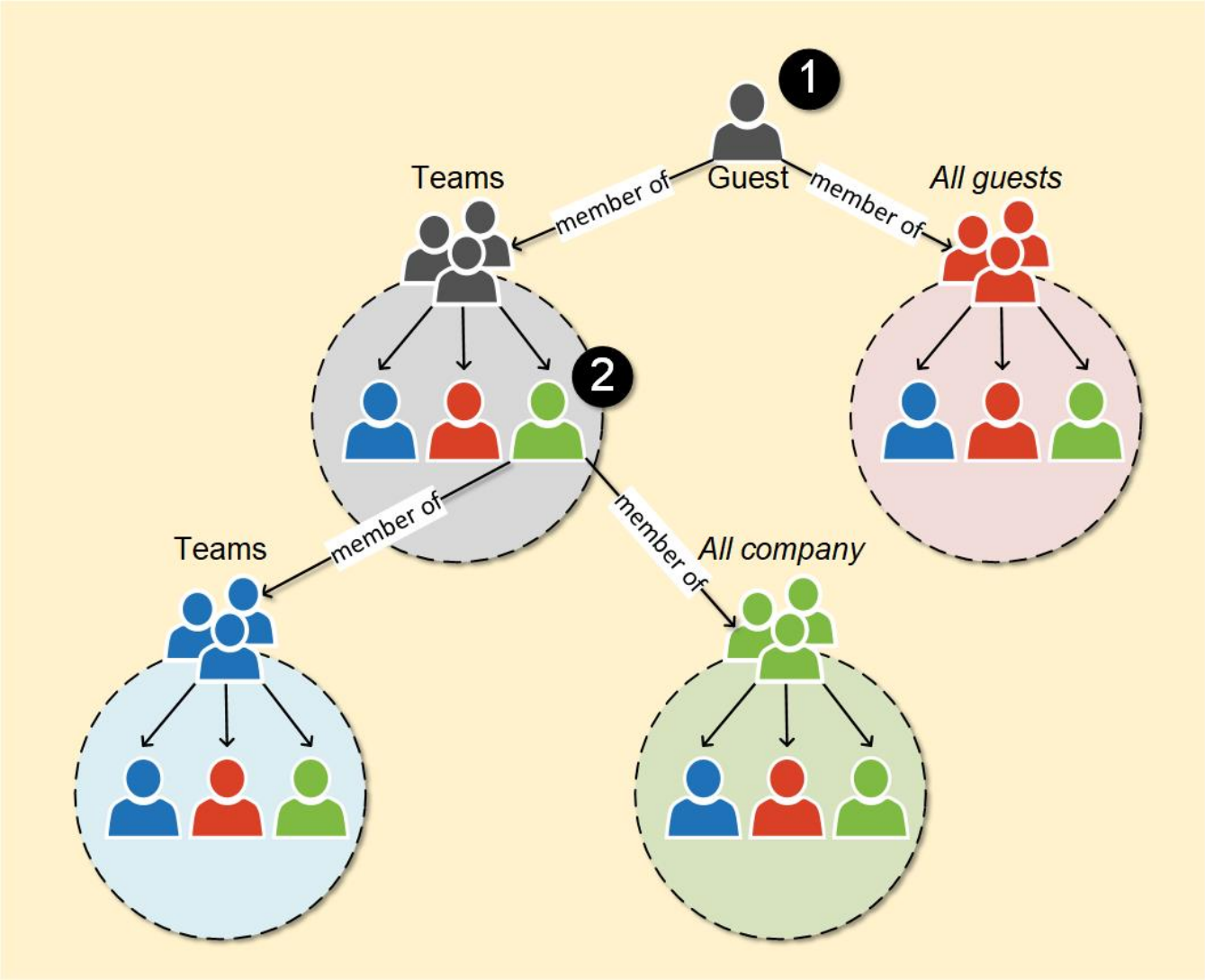
Guest users *

- 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

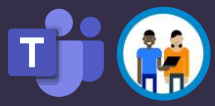
User enumeration

Extracting Teams content as a guest user



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

DEMO!

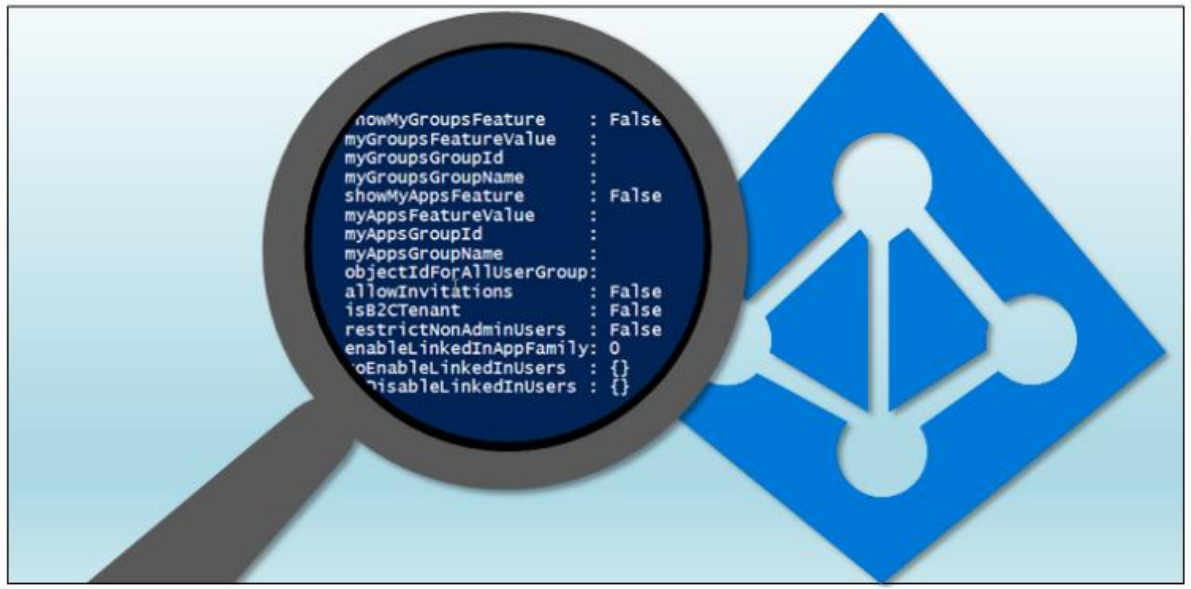


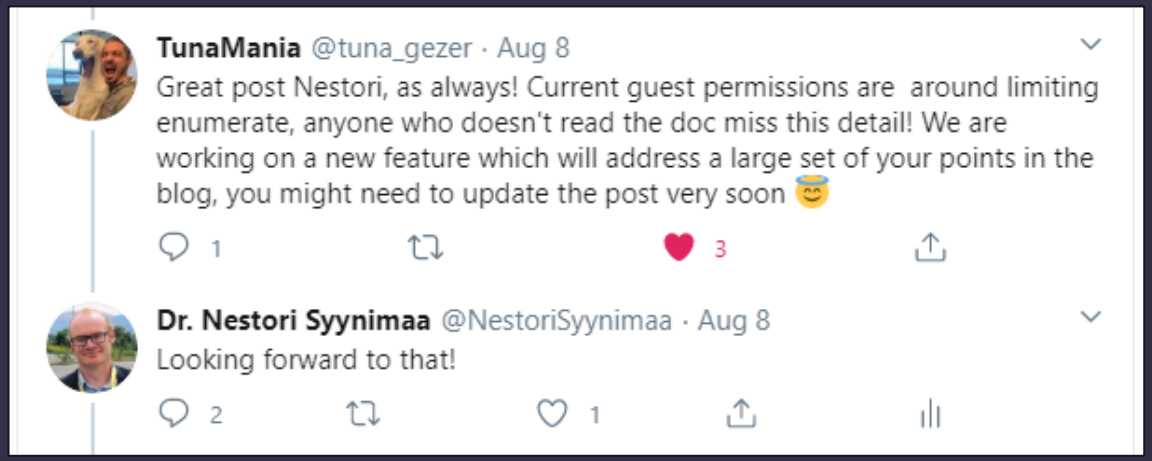
Blogged on August 7th 2020

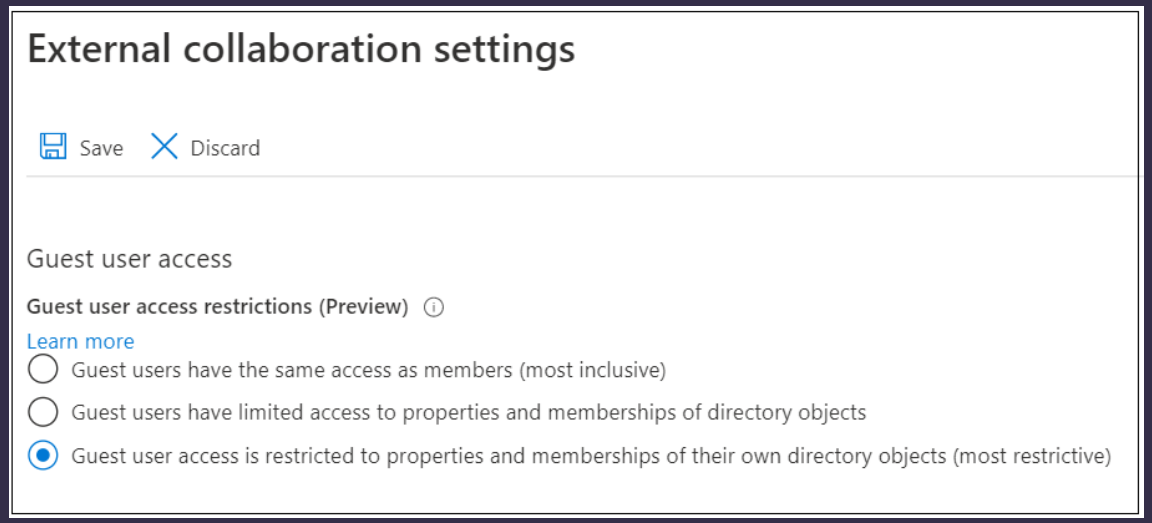
Extracting Teams content as a guest user

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

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

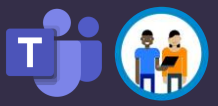






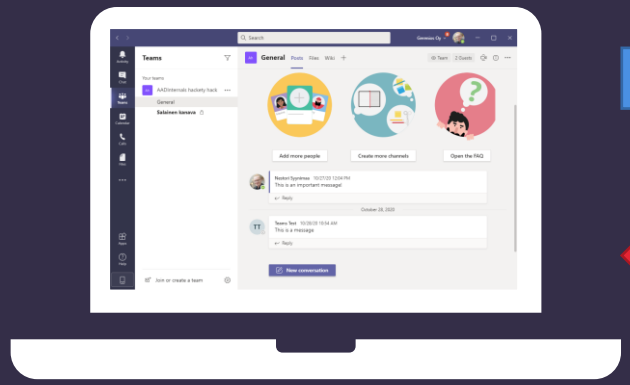
https://o365blog.com/post/quest_for_guest/

Bypassing Teams Security Policies



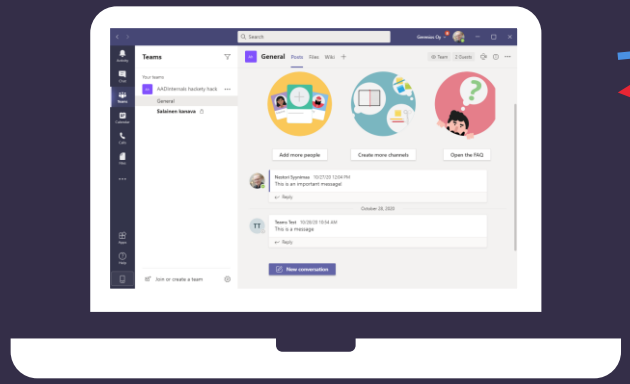
During the Teams start-up

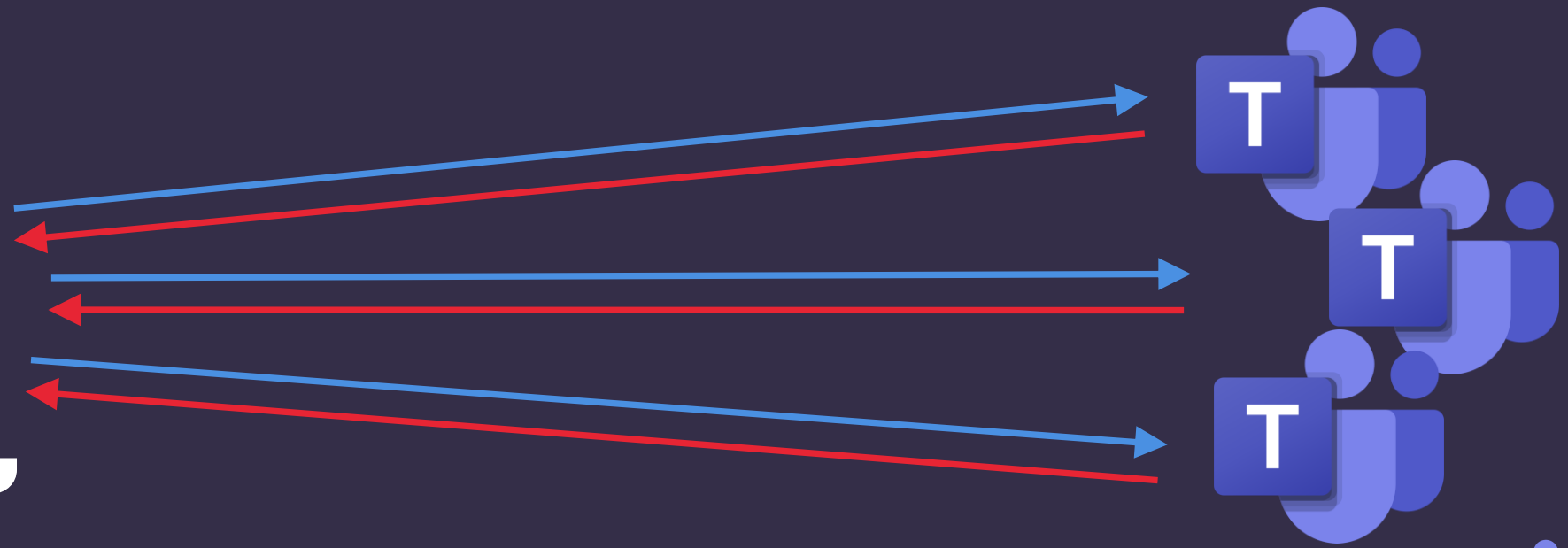
Bypassing Teams Policies



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

messagingPolicy, meetingPolicy, applicationPolicy





Example: messagingPolicy

Bypassing Teams Policies

```
"messagingPolicy": {
    "value": {
        "allowUserEditMessage": false,
        "allowUserDeleteMessage": false,
        "allowUserChat": false,
        "allowGiphy": true,
        "giphyRatingType": "Moderate",
        "allowGiphyDisplay": true,
        "allowPasteInternetImage": true,
        "allowMemes": true,
        "allowStickers": true,
        "allowUserTranslation": true,
        "allowUrlPreviews": true,
        "readReceiptsEnabledType": "UserPreference",
        "allowImmersiveReader": true,
        "allowPriorityMessages": true,
        "audioMessageEnabledType": "ChatsAndChannels",
        "channelsInChatListEnabledType": "DisabledUserOverride",
        "allowRemoveUser": true,
        "allowSmartReply": true
    }
}
```

About client-side “security”

Bypassing Teams Policies

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

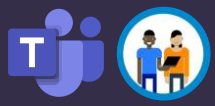
- *" The software is composed of a server that relies on the client to implement a mechanism that is intended to protect the server."*
- *" .. an attacker can modify the client-side behavior to bypass the protection mechanisms.."*

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!

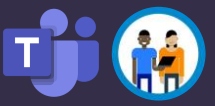


Summary

- 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..?



@DrAzureAD

Rate my session & Calls to Action

Follow me on Twitter!

	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