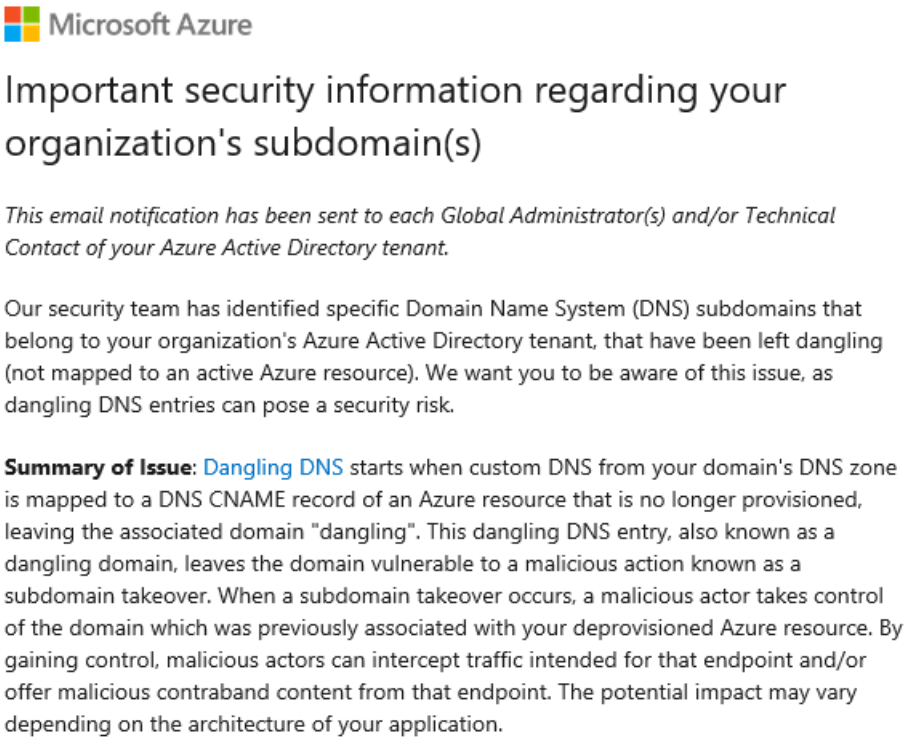
Dangling DNS – Azure

Yesterday, I received alert email from Microsoft on above subject. I was worried. I want to make sure cloud domain and account were not compromised. Download the script provided by Microsoft and tested. No issue with cloud domain or account. Here is what you can do, if you get same alert email from Microsoft.



Microsoft Azure

Important security information regarding your organization's subdomain(s)

This email notification has been sent to each Global Administrator(s) and/or Technical Contact of your Azure Active Directory tenant.

Our security team has identified specific Domain Name System (DNS) subdomains that belong to your organization's Azure Active Directory tenant, that have been left dangling (not mapped to an active Azure resource). We want you to be aware of this issue, as dangling DNS entries can pose a security risk.

Summary of Issue: Dangling DNS starts when custom DNS from your domain's DNS zone is mapped to a DNS CNAME record of an Azure resource that is no longer provisioned, leaving the associated domain "dangling". This dangling DNS entry, also known as a dangling domain, leaves the domain vulnerable to a malicious action known as a subdomain takeover. When a subdomain takeover occurs, a malicious actor takes control of the domain which was previously associated with your deprovisioned Azure resource. By gaining control, malicious actors can intercept traffic intended for that endpoint and/or offer malicious contraband content from that endpoint. The potential impact may vary depending on the architecture of your application.

Install PowerShell 7 and install Azure PowerShell Cmdlet

Do the following:

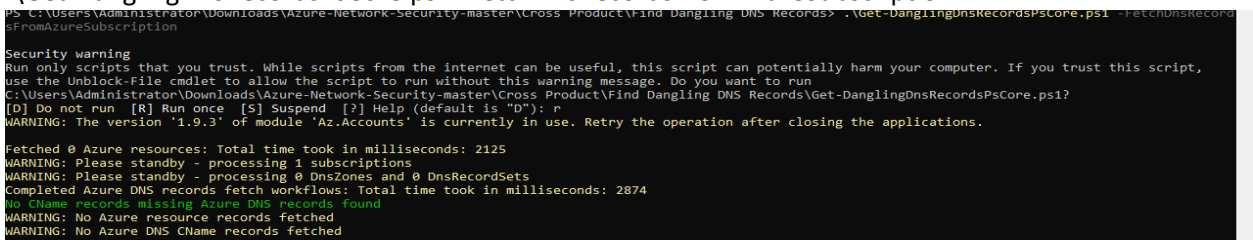
1. Open PS and check PowerShell version - $PSVersionTable.PSVersion
2. Set Execution Policy Unrestricted
3. If you have PS7 then you can run below command. If you have PS5 then upgrade to PS7
4. You will be asked

```
Are you sure you want to install the modules from 'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"):
```

Say (A)

5. Wait for the module to install
6. Connect to Azure with this command Connect-AzAccount
7. After that change directory to where you have Azure script downloaded so you can run the command

8. .\Get-DanglingDnsRecordsPsCore.ps1 -FetchDnsRecordsFromAzureSubscription



9. Once the command completes you should see 0s – if there is anything with Dangling then you need to get in touch with MS to fix the issue asap.

AzureResourceProviderName	AzureResourceCount	AzureCNameMatchingResources	AzureCNameMissingResources
Azure API Management	0	0	0
Azure Container Instance	0	0	0
Azure CDN	0	0	0
Azure Front Door	0	0	0
Azure App Service	0	0	0
Azure Blob Storage	0	0	0
Azure Public IP addresses	0	0	0
Azure Classic Cloud	0	0	0
Azure Traffic Manager	0	0	0

AzureResourceProviderName	AzureResourceCount	AzureCNameMatchingResources	AzureCNameMissingResources	
Azure API Management	0	0	7	(Dangling DNS records needs attent
Azure Container Instance	0	0	7	
Azure CDN	0	0	10	
Azure Front Door	0	0	12	
Azure App Service	0	0	16	
Azure Blob Storage	1	0	24	
Azure Public IP addresses	0	0	7	
Azure Classic Cloud	0	0	0	
Azure Traffic Manager	0	0	0	
Azure Xbox	0	0		

Script Link - https://aka.ms/DanglingDNSDomains

Az Module Install

Using the PowerShellGet cmdlets is the preferred installation method. Install the Az module for the current user only. This is the recommended installation scope. This method works the same on Windows, macOS, and Linux platforms. Run the following command from a PowerShell session:

```
if ($PSVersionTable.PSEdition -eq 'Desktop' -and (Get-Module -Name AzureRM -ListAvailable)) {
    Write-Warning -Message ('Az module not installed. Having both the AzureRM and ' +
     'Az modules installed at the same time is not supported.')
} else {
    Install-Module -Name Az -AllowClobber -Scope CurrentUser
}
```

Thanks

Ram Lan
11th Sep 2020