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.



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

```
PS c:\Users\Administrator\Downloads\Azure-Network-Security-master\Cross Product\Find Dangling DNS Records> .\Get-DanglingDnsRecordsPsCore.ps1 -FetchDnsRecord SfromAzureSubscription

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the Unblock-File condet to allow the script to run without this warning message. Do you want to run

C:\Users\Administrator\Downloads\Azure-Network-Security-master\Cross Product\Find Dangling DNS Records\Get-DanglingDnsRecordsPsCore.ps1?

[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D'): r
WARRINGT The version "1.9.3" of module "2.Accounts" is currently in use. Retry the operation after closing the applications.

Fetched 0 Azure resources: Total time took in milliseconds: 2125
WARRING: Please standby - processing 1 subscriptions
WARRING: Please standby - processing 0 DnsZones and 0 Dns
```

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.

zurekesourceprovidername Az	ureResourceCount Azu	reCNameMatchingResources A	zureCNameMissingResources
zure API Management	0		0
zure Container Instance	0	0	0
zure CDN	0	0	0
zure Front Door	0	0	0
zure App Service	0	0	0
zure Blob Storage	0	0	9
zure Public IP addresses	0	0	0
zure Classic Cloud	0	0	0
zure Traffic Manager	0	0	9
zureResourceProviderName AzureResour	ceCount AzureCNameMatchingRe	esources AzureCNameMissingResources	
zureResourceProviderName AzureResour			/ Dangling DNS records needs atter
zureResourceProviderName AzureResour	ceCount AzureCNameMatchingRe	esources AzureCNameMissingResources 0 7	(Dangling DNS records needs atten
zureResourceProviderName AzureResour zure API Management zure Container Instance			(Dangling DNS records needs atter
cureResourceProviderName AzureResour cure API Management cure Container Instance cure CDN		 0 7 0 7	(Dangling DNS records needs atter
zureResourceProviderName AzureResour zure API Management zure Container Instance zure CDN zure Front Door			(Dangling DNS records needs atter
cureResourceProviderName AzureResour cure API Management cure Container Instance cure CDN cure Front Door cure App Service			(Dangling DNS records needs atter
cureResourceProviderName AzureResourceProviderName AzureResourceProviderName AzureResourceProviderName AzureResourceProviderName AzureResourceProviderName Azure Blob Storage			(Dangling DNS records needs atter
cureResourceProviderName AzureResourceUre API Management cure Container Instance cure CON cure Front Door cure App Service cure Blob Storage cure Public IP addresses cure Classic Cloud			(Dangling DNS records needs atter
zureResourceProviderName AzureResour zure API Management zure Container Instance zure Front Door zure Front Door zure App Service zure Blob Storage zure Public IP addresses zure Classic Cloud zure Traffic Manager		0 7 0 7 0 10 0 11 0 12 0 16 0 24 0 7 0 0	(Dangling DNS records needs atter
			(Dangling DNS records needs atter

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