

- [disque](#)
  - [chiffrement du disque](#)
  - [Initialiser un disque virtuel sur une VM Windows](#)
- [réseaux](#)
  - [Changer une IPv4 Windows](#)
- [terminal powershell](#)
  - [Script](#)
    - [automatisation des msie à jour à chaque démarrage](#)
- [Création de fichier via le Cmd de Windows et les déplacer](#)
- [vérifier que son windows est un botnet ou pas](#)

## disque

### chiffrement du disque

Avec Windows Professionnel, Entreprise, Education

Aller dans Panneau de configuration

Cliquer sur Systeme et sécurité puis sur chiffremnt de lecteur Bitlocker

Activer Bitlocker

choisir le mode de déverrouillage

sauvegarder la clé de Récupération

choisir le mode de chiffrement

cliquer sur démarrer le chiffrement

### Initialiser un disque virtuel sur une VM Windows

Clic droit sur le menu démarrer et gestion des disques>une petite fenetre s'ouvre

cliquer sur ok

Clic droit sur l'espace non alloué puis cliqué sur nouveau volume simple

Cliquer toujours sur suivant

Je personnalise le nom du volume

Cliquer sur suivant et terminer pour tomber sur ça

Quand le disque est formaté il est bleu sinon il est noir

# réseaux

## Changer une IPv4 Windows

aller dans parametre>réseau et internet>propriété (id\_du\_réseau)>parametres IP

cliquer sur modifier

Appuyer sur manuel et adapter la partie réseau de l'adresse IPv4 et du masque du sous réseau de la machine que vous voulez connecter. Mais l'automatique DHCP est mieux car si les 2 machines sont connectées au même réseau les 2 machine ont la même partie réseaux à leur IP et masque

## terminal powershell

### Script

### automatisation des msie à jour à chaque démarrage

Va dans Windows Powershell ISE> dans la zone blanche de saisi rentre ce script

```
# =====
# Script PowerShell : Mise à jour automatique
# Auteur : [Ton Nom]
# =====

# Exécuter avec élévation (admin)
if (-not ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Princip
al.WindowsBuiltInRole] "Administrator")) {
    Start-Process powershell "-ExecutionPolicy Bypass -File
`"$PSCommandPath`" -Verb RunAs
    exit
}

# Active Windows Update module (nécessite PSWindowsUpdate)
if (-not (Get-Command Get-WindowsUpdate -ErrorAction SilentlyContinue)) {
    Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force
    Install-Module PSWindowsUpdate -Force -Confirm:$false
}

Import-Module PSWindowsUpdate

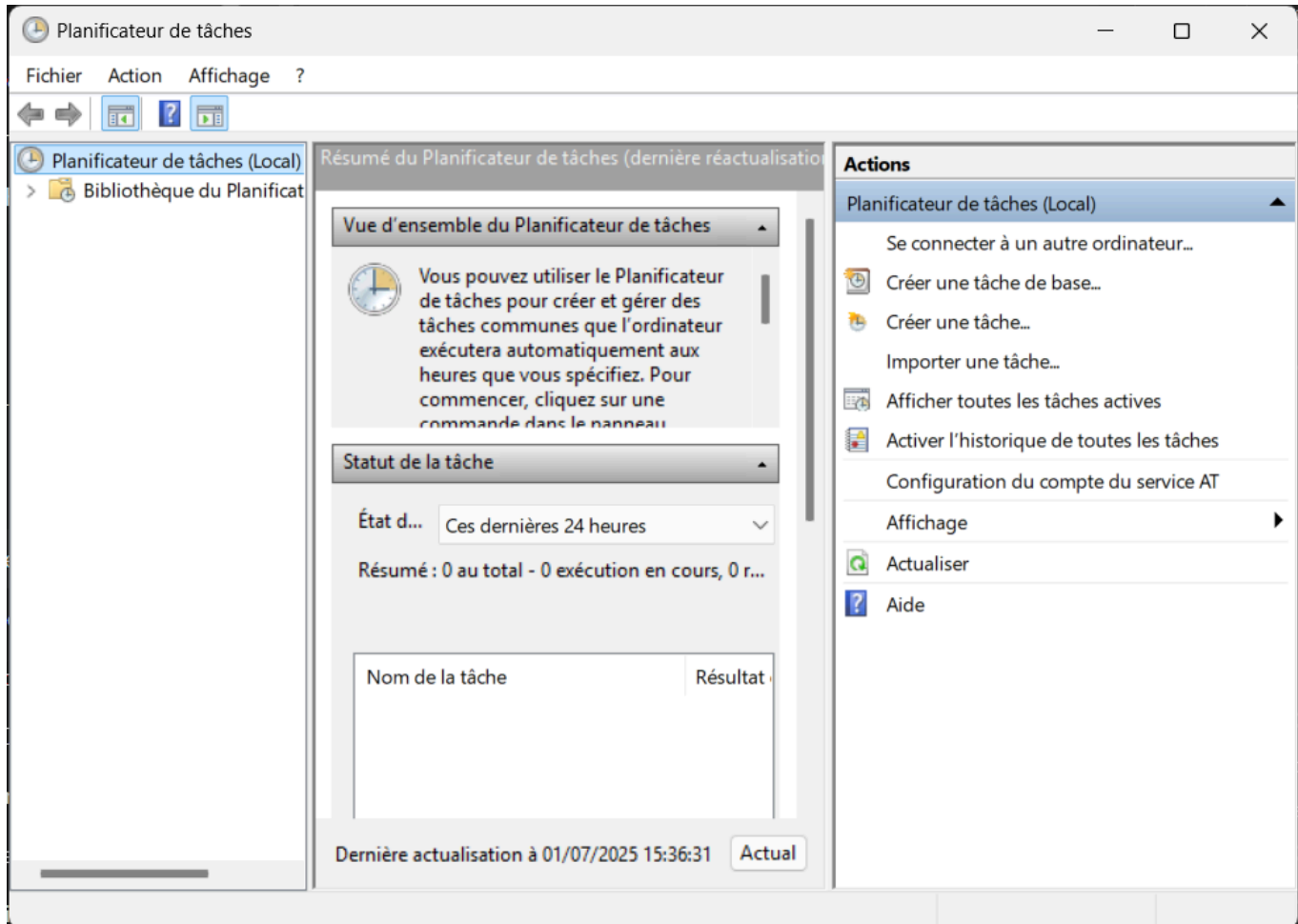
# Rechercher et installer les mises à jour automatiquement
```

```
Write-Output "Recherche des mises à jour en cours..."
Get-WindowsUpdate -AcceptAll -Install -AutoReboot -Verbose
```

enregistre le sous le nom par exemple de MiseAJour-Auto.ps1

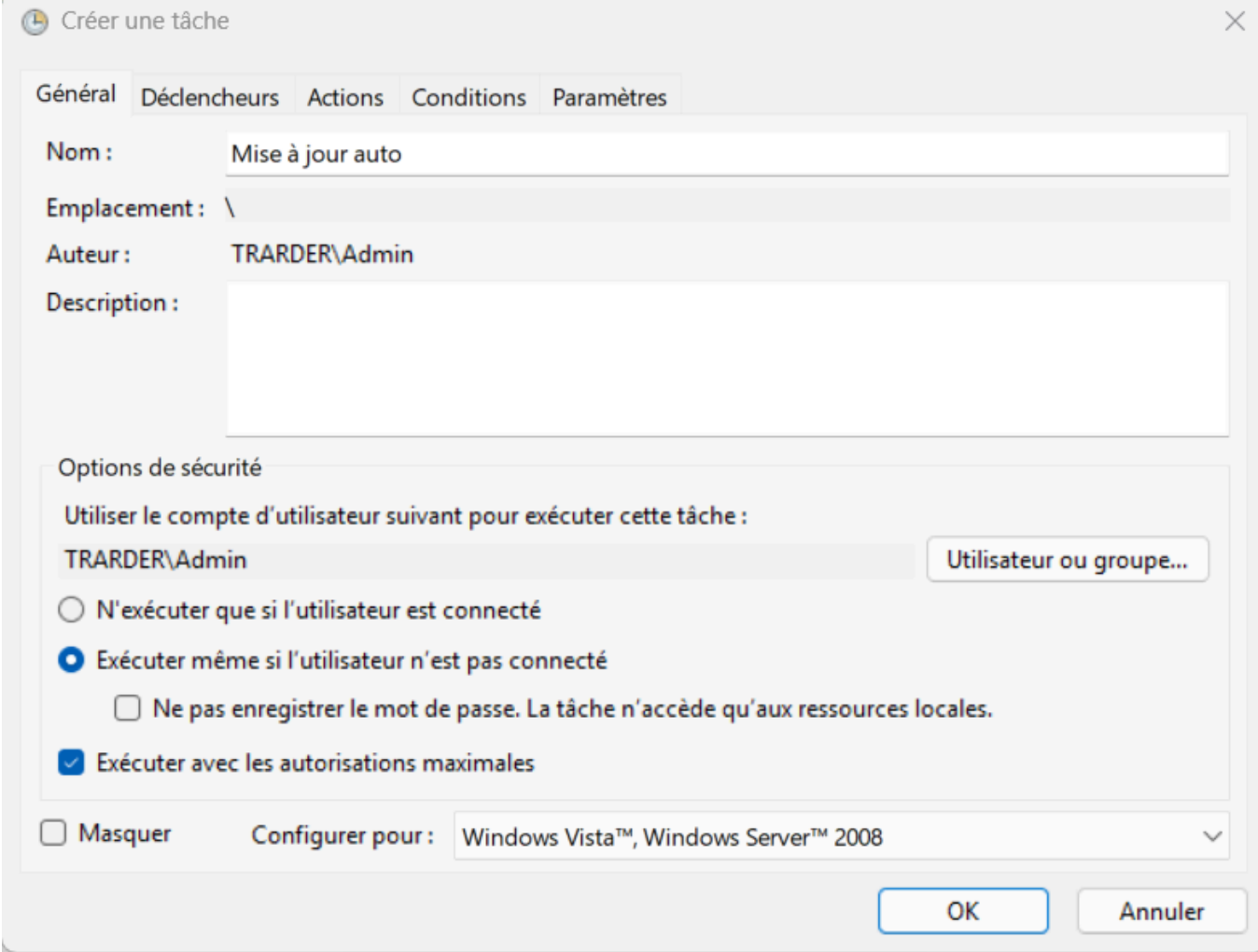
exécute le une fois en tant qu'admin en cliquant sur la fleche verte

Ouvre le planificateur de tâche



cliquer sur créer une tâche

Définir la tâche comme ci dessous



The image shows the 'Créer une tâche' (Create Task) dialog box in Windows Task Scheduler. The 'Général' (General) tab is selected. The task name is 'Mise à jour auto'. The location is '\'. The author is 'TRARDER\Admin'. The description field is empty. Under 'Options de sécurité' (Security options), the task is configured to run using the 'TRARDER\Admin' user. The options are: 'N'exécuter que si l'utilisateur est connecté' (Not selected), 'Exécuter même si l'utilisateur n'est pas connecté' (Selected), 'Ne pas enregistrer le mot de passe. La tâche n'accède qu'aux ressources locales.' (Not selected), and 'Exécuter avec les autorisations maximales' (Selected). The 'Masquer' (Hide) checkbox is not selected. The 'Configurer pour' (Configure for) dropdown is set to 'Windows Vista™, Windows Server™ 2008'. The 'OK' and 'Annuler' (Cancel) buttons are at the bottom right.

Créer une tâche

Général Déclencheurs Actions Conditions Paramètres

Nom : Mise à jour auto

Emplacement : \

Auteur : TRARDER\Admin

Description :

Options de sécurité

Utiliser le compte d'utilisateur suivant pour exécuter cette tâche :

TRARDER\Admin Utilisateur ou groupe...

☐ N'exécuter que si l'utilisateur est connecté

☒ Exécuter même si l'utilisateur n'est pas connecté

☐ Ne pas enregistrer le mot de passe. La tâche n'accède qu'aux ressources locales.

☒ Exécuter avec les autorisations maximales

☐ Masquer Configurer pour : Windows Vista™, Windows Server™ 2008

OK Annuler

dans la rubrique déclencheur cliquer sur nouveau

Nouveau déclencheur

Lancer la tâche :

Au démarrage

Paramètres

Aucun autre paramètre n'est requis.

Paramètres avancés

☐ Reporter la tâche pendant :

15 minutes

☐ Répéter la tâche toutes les :

1 heure

☐ Arrêter toutes les tâches à l'issue de la durée de répétition

☐ Arrêter la tâche si elle s'exécute plus de :

1 jour

☐ Activer :

01/07/2025

15:45:06

☐ Expiration :

01/07/2026

15:45:06

☒ Activée

☐ Synch. fuseaux horaires

☐ Synch. fuseaux horaires

OK

Annuler

Nouvelle action ✕

Vous devez spécifier l'action que cette tâche effectuera.

Action : Démarrer un programme ▾

Paramètres

Programme/script :  
C:\Users\Admin\Documents\MiseAJour-Auto.ps1 Parcourir...

Ajouter des arguments (facultatif) : "C:\Scripts\MiseAJour-Au"

Commencer dans (facultatif) :

OK Annuler

ajouter le chemin du fichier script dans les argument

```
-ExecutionPolicy Bypass -File "C:\Scripts\MiseAJour-Auto.ps1"
```

Cliquer sur OK

et la il sera mis dans la bibliothèque du planificateur de tache

## Création de fichier via le Cmd de Windows et les déplacer

---

```
Microsoft Windows [version 10.0.20348.169]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>echo "Hello World!" > test1.txt
C:\Users\Administrateur>echo "Hello World!" > test2.txt
C:\Users\Administrateur>echo "Hello World!" > test3.txt
C:\Users\Administrateur>echo "Hello friends" > test01.txt
C:\Users\Administrateur>echo "Hello friends" > test02.txt
C:\Users\Administrateur>echo "Hello friends" > test03.txt
C:\Users\Administrateur>move test1.txt Raid1
1 fichier(s) déplacé(s).
C:\Users\Administrateur>move test2.txt Raid0
1 fichier(s) déplacé(s).
C:\Users\Administrateur>move test3.txt Raid5
1 fichier(s) déplacé(s).
```

Pour désactiver un disque dans un Raid aller dans gestionnaire de disque clic gauche sur un disque pour mettre hors connexion

## vérifier que son windows est un botnet ou pas

```
#netstat
ouvrir un terminal en mode admin
taper netstat -anob #rechercher des connexion étrangeou multiple
vers des IP distante
copier adresse IP en question et le mettre sur whois.domaintools.com ou
abuseip.com
#scan spécialisé et gratuit comme PQUALITYSCORE (3ieme lien en dessous)
le site affiche votre IP confirmer en recopiant IP donné dans le champ
check
```

site: whois.domaintools.com

abuseip.com

<https://tinyurl.com/ipquality>

## Bot Detection Test for 37.67.92.59

Not a Bot - Bot Connection NOT Detected!

**37.67.92.59** (59.92.67.37.rev.sfr.net) has not been detected as a **bot**. We have not identified any bot activity from this IP address.

### Check Bot Status for 37.67.92.59

IP Address	<b>37.67.92.59</b>
Bot Detection	 <b>Clean IP – Not A Bot</b> This IP address is not a Bot.
Proxy & VPN Detection	 <b>Proxy Detected</b> This IP address is a Proxy Connection.
Risk Status	<b>83% – Abusive IP</b>
ISP	<b>SFR</b>
Country	<b>FR</b> 
City	<b>Toul</b>
CIDR IP Address Subnet	<b>37.67.92.0/24</b>

[Perform a Full IP Address Lookup on 37.67.92.59](#)

View additional IP address details like VPN provider, Risk Scores, and geographic location data.

Signe qu'on est devenu un botnet

- Ralentissement inhabituel du système ou de la co internet
- Activité réseau anormal même lorsque vous n'utilisez pas activement internet
- Présence de processus inconnu dans le gestionnaire de tâche
- comportement bizarre du système (redemmarage non attendu, message d'erreur inhabituel)