



USB Storage Restriction bypass

SSTIC 2026 - RUMP

04/06/2026

Restriction d'utilisation de supports de stockage de masse USB

- **Durcissement Windows**
- **Solution DLP**
 - Data Loss Prevention

Pourquoi les contourner ?

- Importer des outils
- Récupérer nos traces pour les rapports
- Pour le fun !

- **Machine virtuelle**

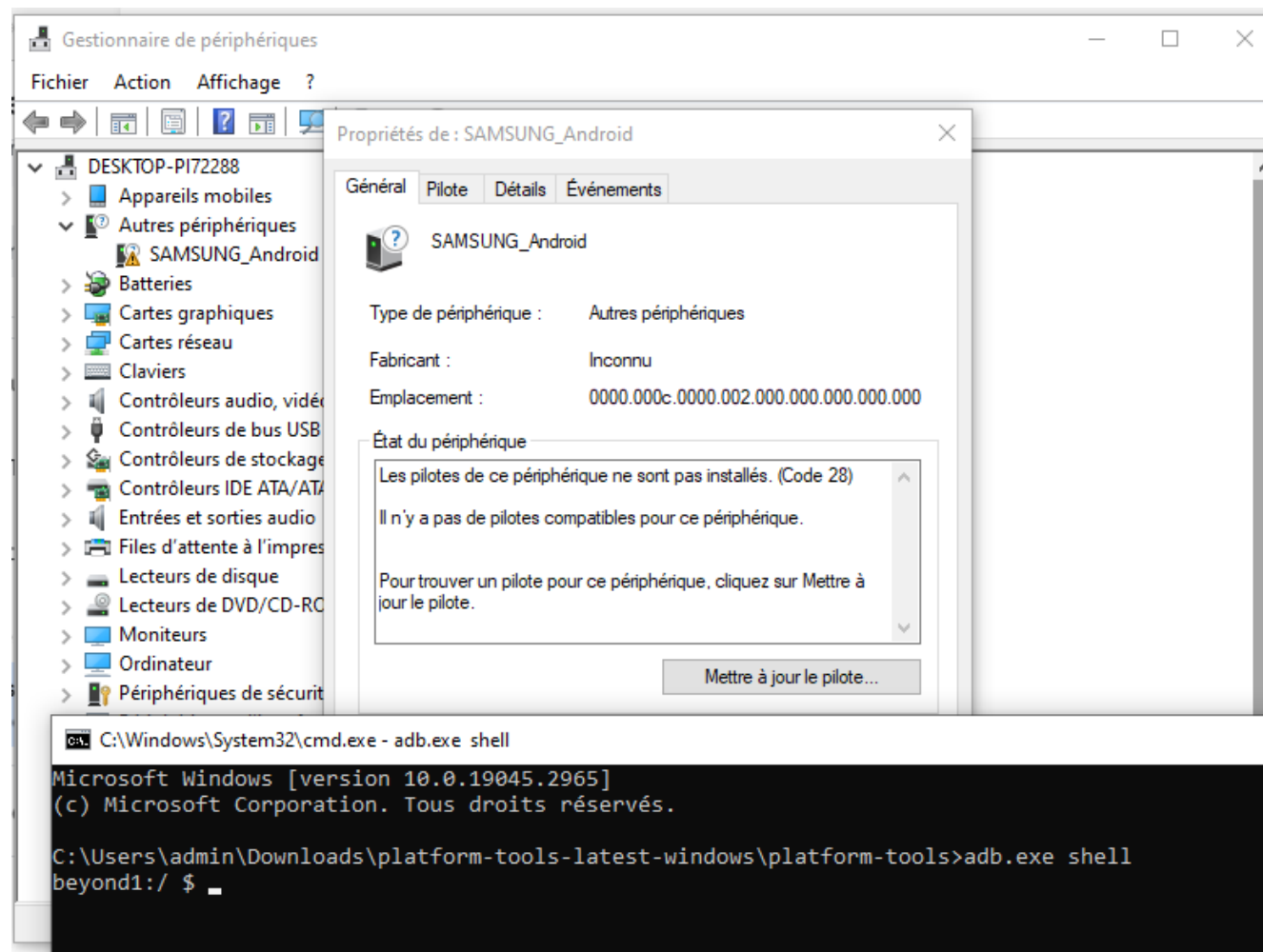
- Partager un répertoire avec la VM
- Monter la clé USB sur la VM
- Limites
 - Nécessite un système de virtualisation préinstallé ou des droits d'admin locaux

- **Les supports "autres"**

- WPD (Windows Portable Device)
- Lecteur / Graveur de CD/DVD
- Lecteur de disquette (ZIP)
- Limites
 - Matériel à avoir avec soi

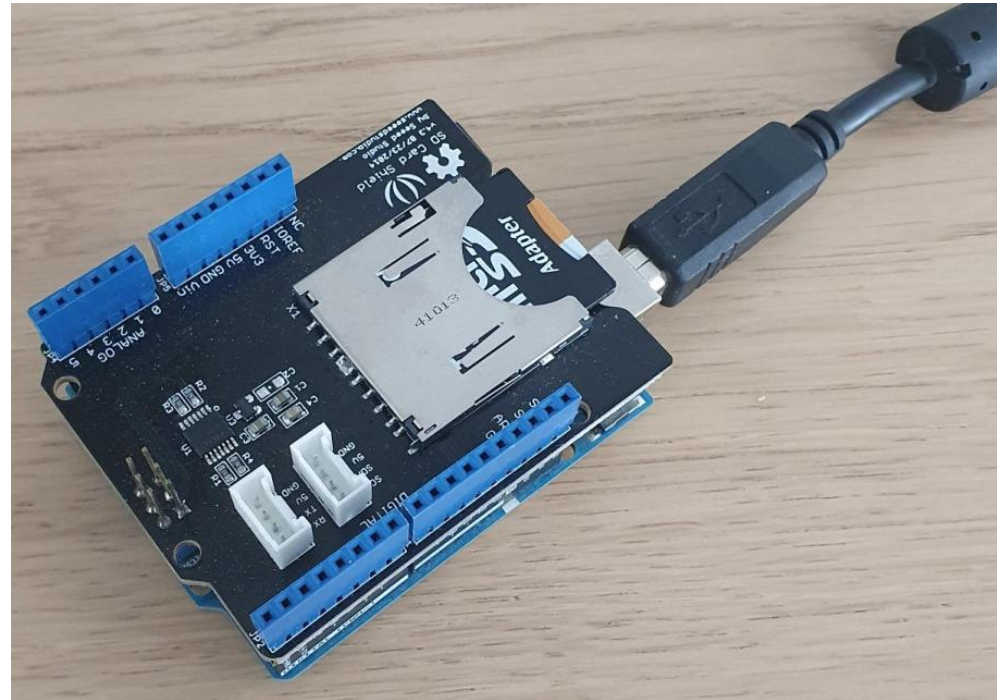
- **Intégré à la machine** ou **Dongle USB**
 - Transfert de fichiers natif à Windows
 - <https://github.com/gryfman/DLPwn>

- **ADB (Android Debug Bridge)**
 - Dans ce mode le téléphone n'est pas considéré comme un support de masse
- **Limite**
 - Nécessite d'importer ADB
 - <https://developer.android.com/tools/releases/platform-tools>



Câble série - Arduino

- **Arduino + Shield USB**



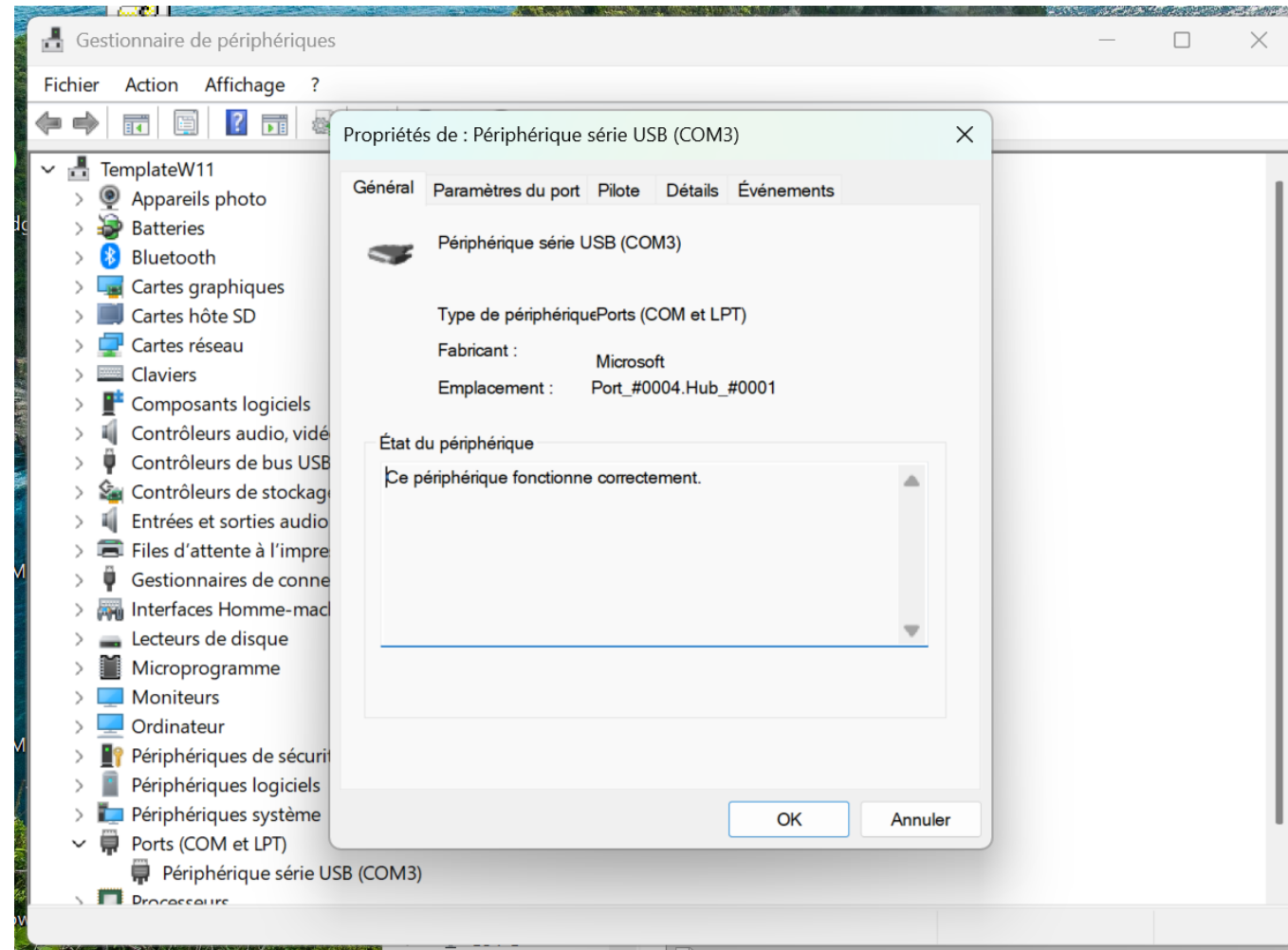
- **Arduino + Shield USB**

- Liaison série sur USB
- Code permettant d'exfiltrer des fichiers via la liaison série
 - https://github.com/cervoise/arduino_usb_key/

```
$portName = "COM3"  
$baudRate = 9600
```

```
$port = New-Object System.IO.Ports.SerialPort $portName, $baudRate, None, 8, one  
$port.Open()
```

Câble série - Arduino





<https://www.linkedin.com/company/synacktiv>



<https://x.com/synacktiv>



<https://bsky.app/profile/synacktiv.com>



<https://synacktiv.com>

Un incident ? Contactez csirt@synacktiv.com.