Documentation technique

Module d'extraction de l'historique USB

Identification des supports amovibles connectés à un poste Windows

Type de document	Documentation technique
Sujet	Module d'extraction de l'historique USB
Technologie	PowerShell / Windows Plug and Play
Classes auditées	USBSTOR et WPD
Sortie générée	Rapport HTML sous forme de tableau de bord
Public cible	Administrateurs système / support / sécurité

Résumé

Ce document présente le fonctionnement d'un script PowerShell dédié à l'investigation des périphériques USB. Il explique comment les informations conservees par Windows permettent d'identifier les supports de stockage et appareils mobiles connectés, meme lorsqu'ils ne sont plus physiquement présents sur la machine.

1. Objectif

Dans le cadre de la sécurisation d'un poste de travail, le controle des supports amovibles est un point sensible. L'objectif du module est d'apporter une capacité d'investigation numerique permettant de lister les périphériques USB ayant déjà été connectés à la machine.

Cette verification reste utile meme lorsque le support n'est plus branché au moment de l'audit, car Windows conserve des traces persistantes de certains périphériques détectés par le service Plug and Play.

Objectif principal

Fournir un historique lisible des clés USB, disques externes, smartphones et tablettes connectés au poste, afin de faciliter l'analyse sécurité et la recherche d'eventuelles exfiltrations de données.

2. Principe technique

Lorsqu'un périphérique USB est branché pour la première fois, Windows cree des entrees persistantes dans la base de registre. Les périphériques de stockage de masse sont notamment répertoriés dans la classe USBSTOR.

Plutôt que de parcourir manuellement la base de registre avec regedit, le script exploite les commandes natives PowerShell liées au Plug and Play, principalement Get-PnpDevice et Get-PnpDeviceProperty.

1. Détection	2. Extraction	3. Horodatage	4. Rapport
Interrogation des périphériques connus par Windows.	Récupération du modèle, constructeur et numéro de série.	Lecture des dates de première et dernière installation.	Génération d'un tableau de bord HTML exploitable.

3. Informations collectees

Le script extrait les informations utiles à l'identification et au suivi des périphériques détectés par Windows.

Information	Source technique	Utilité
Modèle / Description	Propriétés de l'objet PnP	Identifier le type de support connecté.
Constructeur	Propriétés de l'objet PnP	Associer le support à un fabricant.
Numéro de série unique	Analyse de la chaine InstanceId	Distinguer deux périphériques de meme modèle.
Date de première connexion	DEVPKEY_Device_FirstInstallDate	Connaître la première détéction par le système.
Date de dernière interaction	DEVPKEY_Device_InstallDate	Évaluer la dernière activite connue.

4. Détection éténdue des appareils mobiles

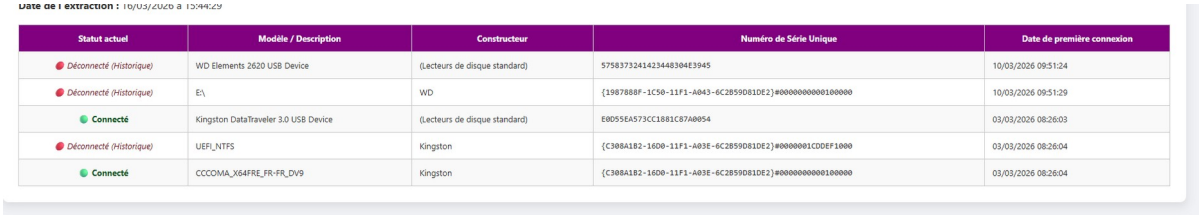
Une recherche limitée à la classe USBSTOR permet d'identifier les supports de stockage classiques, mais elle peut manquer une catégorie importante de périphériques : les smartphones et tablettes connectés en USB.

Ces appareils utilisent souvent le protocole MTP et sont rattaches à la classe WPD, pour Windows Portable Devices. Le script a donc été enrichi afin d'auditer simultanement les classes USBSTOR et WPD.

> **Point de vigilance sécurité**
>
> Les smartphones peuvent représenter un vecteur d'exfiltration de données. Leur prise en compte dans l'audit permet d'obtenir un historique plus complet et plus pertinent pour l'analyse forensique.

5. Rapport généré

Les données collectees sont compilees dans un rapport HTML présente sous forme de tableau de bord. Ce format facilite là lecture, le partage et l'archivage des résultats d'audit.



Statut actuel	Modèle / Description	Constructeur	Numéro de Série Unique	Date de première connexion
Déconnecté (Historique)	WD Elements 2620 USB Device	(Lecteurs de disque standard)	575837324142344830 4E3945	10/03/2026 09:51:24
Déconnecté (Historique)	E:\	WD	{1987888F-1C50-11F1-A043-6C2859D81DE2}#0000000000100000	10/03/2026 09:51:29
Connecté	Kingston DataTraveler 3.0 USB Device	(Lecteurs de disque standard)	E0D55EA573CC1881C87A0054	03/03/2026 08:26:03
Déconnecté (Historique)	UEFI_NTFS	Kingston	{C308A1B2-16D0-11F1-A03E-6C2859D81DE2}#0000001CDDEF1000	03/03/2026 08:26:04
Connecté	CCCOMA_X64FRE_FR-FR_DV9	Kingston	{C308A1B2-16D0-11F1-A03E-6C2859D81DE2}#0000000000100000	03/03/2026 08:26:04

Exemple de rapport : statut, modèle, constructeur, numéro de série et date de première connexion.

Lecture du statut

Le statut Connecté indique qu'un périphérique est actuellement visible par Windows. Le statut Deconnecté (Historique) indique qu'il n'est plus branché, mais que ses informations restent conservees par le système.

6. Validation et cas de test

Le fonctionnement du script a été valide sur une machine virtuelle à l'aide du protocole suivant :

1. Connectér une clé USB physique à la machine.
2. Exécuter le script et verifier que la clé apparait avec le statut Connecté.
3. Éjecter proprement la clé, puis la deconnectér physiquement.
4. Relancer le script et verifier que la clé apparait toujours dans le rapport avec le statut Deconnecté (Historique).
5. Contrôler que le modèle, le numéro de série et les dates de connexion sont conserves.

Résultat attendu

Lorsqu'un périphérique est branché, le rapport doit indiquer le statut Connecté. Après éjection et retrait physique, le même périphérique doit rester visible dans l'historique avec le statut Déconnecté (Historique), ce qui confirme la conservation des traces.

7. Points forts

- Exploitation de commandes PowerShell natives et lisibles.
- Collecte des informations essentielles pour l'investigation USB.
- Détection des supports de stockage et des appareils mobiles.
- Conservation de l'historique meme apres déconnexion physique.
- Génération d'un rapport HTML clair et exploitable.

8. Ameliorations possibles

- Ajouter un export CSV en complement du rapport HTML.
- Integrer un horodatage automatique dans le nom du fichier de sortie.
- Prevoir une signature ou un hash du rapport pour renforcer la traçabilité.
- Ajouter un mode silencieux pour une execution automatisée.
- Filtrer les résultats par constructeur, statut ou date de connexion.
- Ajouter un résumé en fin de rapport avec le nombre de périphériques connectés et historiques.

9. Conclusion

Ce module renforce les capacités d'audit d'un poste Windows en fournissant une vision claire des périphériques USB et appareils mobiles ayant été connectés. Il facilite l'analyse forensique, la recherche de comportements a risque et la documentation des controles de sécurité.

Synthese

Le module permet de passer d'une recherche manuelle et partielle dans la base de registre à un rapport automatisé, structuré et directement exploitable.