

RESINFO - GROUPE DE TRAVAIL **SWMB**

Gabriel MOREAU - Coordinateur

24-26 octobre 2023 / Sète



SWMB (Secure Windows Mode Batch)

- Comité de pilotage : Gabriel MOREAU, Olivier DE MARCHI (LEGI), Clément DEIBER (DR11)
- Besoin de sécuriser Microsoft Windows 10 (et bientôt 11)
- Outil modulaire avec des règles et des anté-règles
- Outil en production sur le LEGI et déployé *a minima* sur quelques sites
- Règle particulière pour chiffrer les disques
- Packaging setup.exe, OCS, WAPT, PDQ Deploy
- 29 personnes sur la liste swmb-gt du GT (+2)

Objectifs prévus en 2023 ↔ non réalisé

- Améliorer les pages du GT sur le site RESINFO
- Plus communiquer sur la liste ASR
- Plus de sites en production avec SWMB
- Plus de règles actives par défaut
- Être plus réactif sur les alertes de sécurité (groupe plus élargi)
- Intégration du pare-feu Windows ?
- Monter des ateliers en visio de prise en main de l'outil

↪ Pas regardé le planning entre deux COPIL...

↪ Incompatible avec monter une ANF (ILAS) de A à Z pour septembre !

Cependant...

- Quelques échanges de courriel sur la liste en 2023
- Un séanca pour expliquer le fonctionnement interne de SWMB au printemps
- Relance effective du GT début septembre 2023
- Une refonte de l'interface graphique
- Ajout de règles de suppression de logiciel
- Un projet d'architecture client-serveur via des **webhooks** !

The image shows two windows side-by-side. The left window is the SWMB application interface, titled 'SWMB: Secure Windows Mode Batch / 7 hours, 46 min'. It features a 'BitLocker' section with 'Status: Running / \\\tAs128', buttons for 'Crypt all Disks with BitLocker' and 'Suspend', and a 'Run Task Schedule Now' section with buttons for 'Boot', 'Post Install', and 'Logon'. At the bottom, it shows 'Version: 3.14.13.0', 'New release available', 'View All Software', and an 'Exit' button. A large SWMB logo is in the center. The right window is a Windows registry viewer titled 'LocalMachine and CurrentUser Software : 10/20/2023 18:44:03'. It displays a table of software entries with columns for Hive, DisplayName, Publisher, DisplayVersion, KeyProduct, and UninstallExe.

Hive	DisplayName	Publisher	DisplayVersion	KeyProduct	UninstallExe
HKLM	XnView MP (x64)	Pierre-e Gougelet	1.6.1.0	XnView MP...	"C:\Program Files\XnViewMP\unins001.exe"
HKLM	XnViewMP 1.5.5	Gougelet Pierre-e	1.5.5	XnViewMP...	"C:\Program Files\XnViewMP\unins000.exe"
HKLM	Xournal++ 1.2.2	Xournal Team	1.2.2	Xournal++	C:\Program Files\Xournal++\uninstall.bat
HKLM	Zoom (32-bit)	Zoom	5.16.22807	{ABB9F849...	MsiExec.exe /X{ABB9F849-684E-4710-BD74-66506
HKLM	Zotero	Corporation for Digital Sch...	6.0.27	Zotero 6.0....	C:\Program Files (x86)\Zotero\uninstall\helper.exe
HKU	balenaEtcher 1.18.8	Balena Ltd.	1.18.8	d2f3b6c7-6...	"C:\WINDOWS\system32\config\systemprofile\Ap
HKU	ideaMaker 4.3.3.6560	Raise3D	4.3.3.6560	ideaMaker	"C:\Program Files\Raise3D\ideaMaker\uninstall.lex
HKU	Picocrypt (Current user)	Evan Su	1.33	EvanSu.Pic...	"C:\Program Files\Picocrypt\unins000.exe"
HKU	SSHFS-Win Manager	Evandro Araujo	1.3.1	b80d7a5d-...	"C:\WINDOWS\system32\config\systemprofile\Ap
HKU	Teleoram Desktoo	Teleoram FZ-LLC	4.8.3	{53F49750-...	"C:\Prooram Files\Teleoram Desktoo\unins000.exe

**Merci à toutes les personnes et entités
nous ayant aidés ou ayant participé depuis le début**

Cette présentation est sous : LICENCE ART LIBRE

<http://artlibre.org/>

