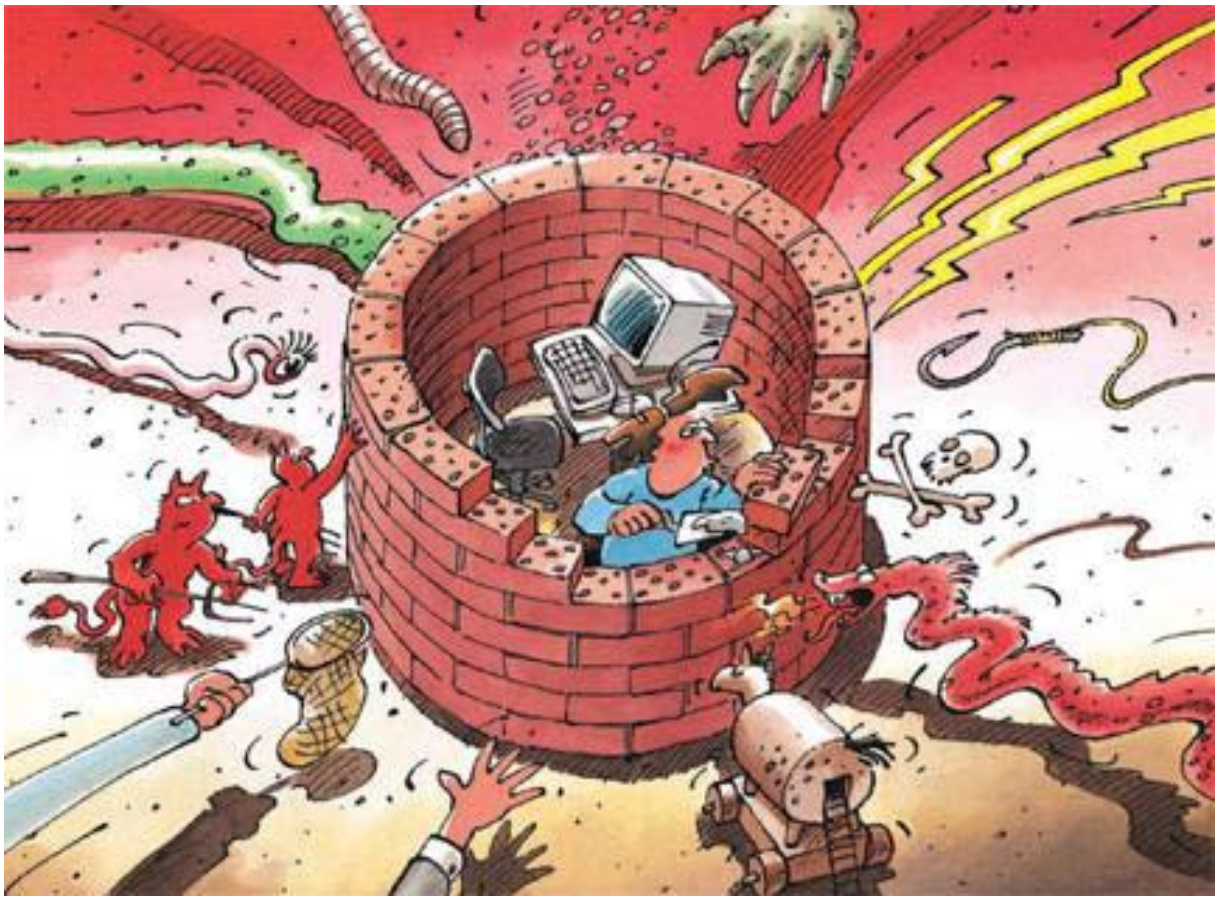
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Informatikstrategieorgan Bund ISB
Nachrichtendienst des Bundes NDB

Melde- und Analysestelle Informationssicherung MELANI
www.melani.admin.ch

Déblocage du PC infecté par un maliciel qui exige un payement

Version 1.1

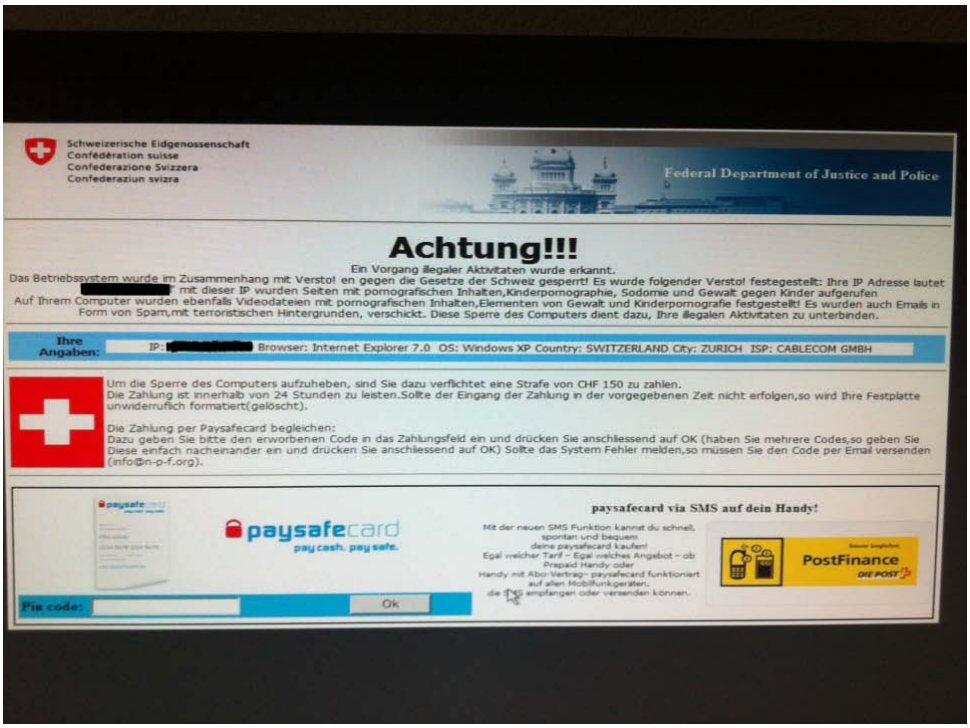


La Centrale d’analyse et de prévention MELANI a été informée du fait qu’un maliciel est en circulation. Ledit bloque toute fonction de l’ordinateur. Une fenêtre s’affiche à l’écran avec un message qui semble provenir du Département fédéral de justice et police. Le message exige que l’utilisateur de l’ordinateur s’acquitte d’une amende 150 CHF, sous le prétexte que du matériel illégal a été retrouvé sur son ordinateur.

Dans ce qui suit, il est expliqué comment annuler ce blocage et redémarrer l’ordinateur.

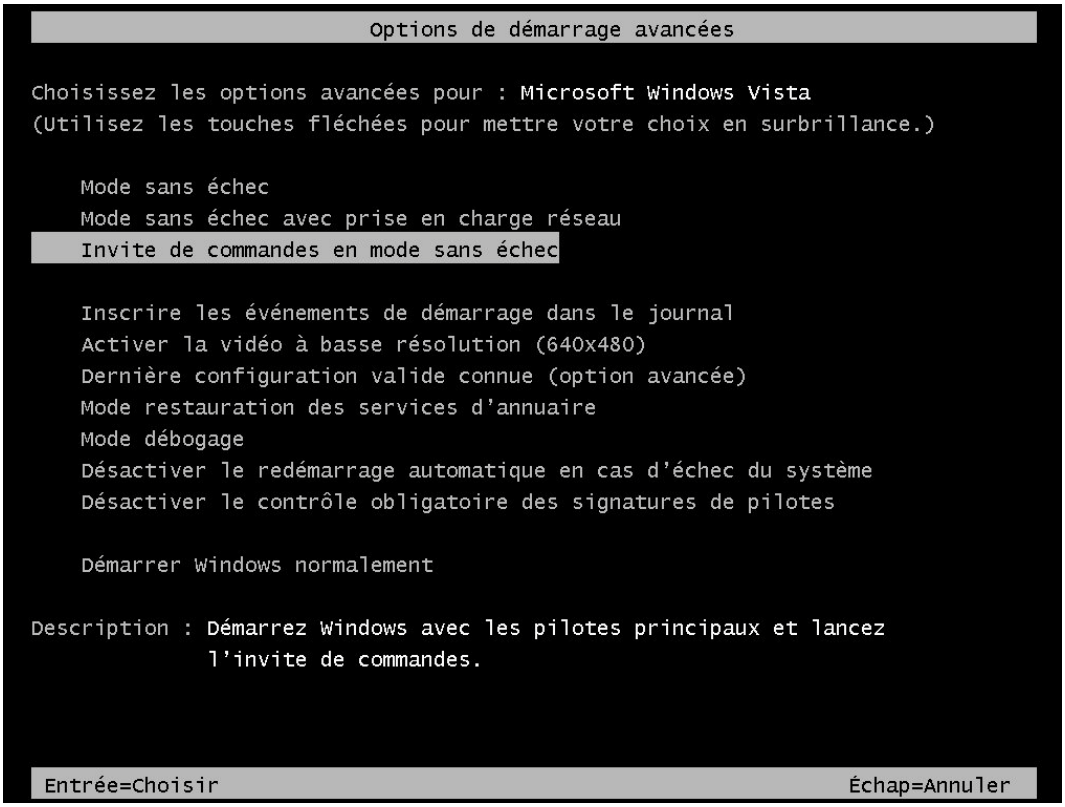
Après avoir débloqué avec succès votre ordinateur et avoir sauvegardé les données, il est conseillé de réinstaller le système.

Veuillez faire attention au fait que ce déblocage est sans aucune garantie. MELANI ne peut pas être retenue responsable d’éventuels dommages générés par la procédure décrite dans ce document. MELANI ne fournit aucun support ultérieur.



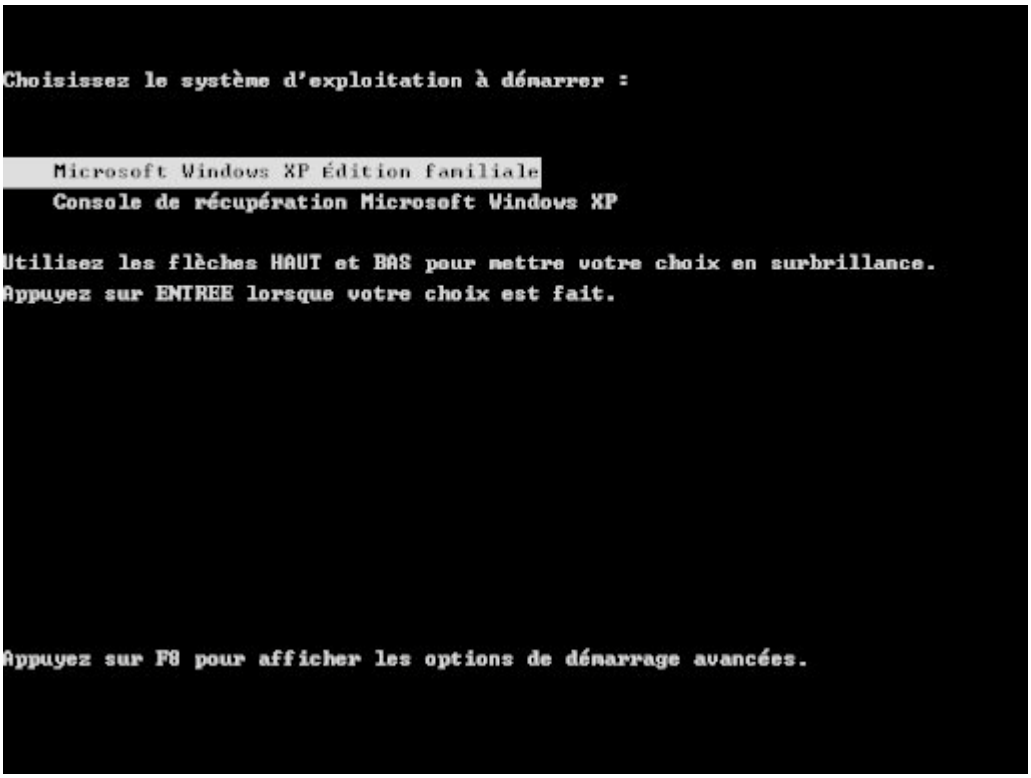
Phase 1:

Démarrez votre ordinateur et appuyez sur la touche F8 jusqu’à ce que le menu « Options de démarrage avancées » s’affiche. Dans le menu, choisissez « Invite de commandes en mode sans échec » :



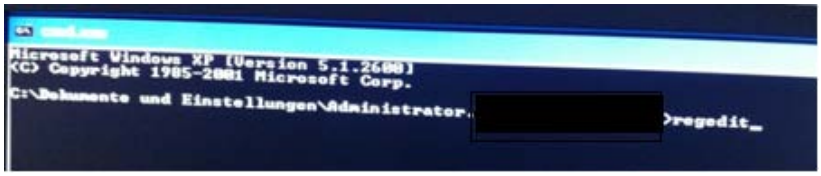
Phase 2

Choisissez le système d’exploitation à démarrer, par exemple « Microsoft Windows XP Edition familiale » :



Phase 3

Eventuellement, faut-il encore s’identifier (il est mieux de le faire sous le compte Administrateur) et une fenêtre de console s’ouvre à ce moment-là. Ici, il faut écrire « regedit » et cliquer sur Enter.



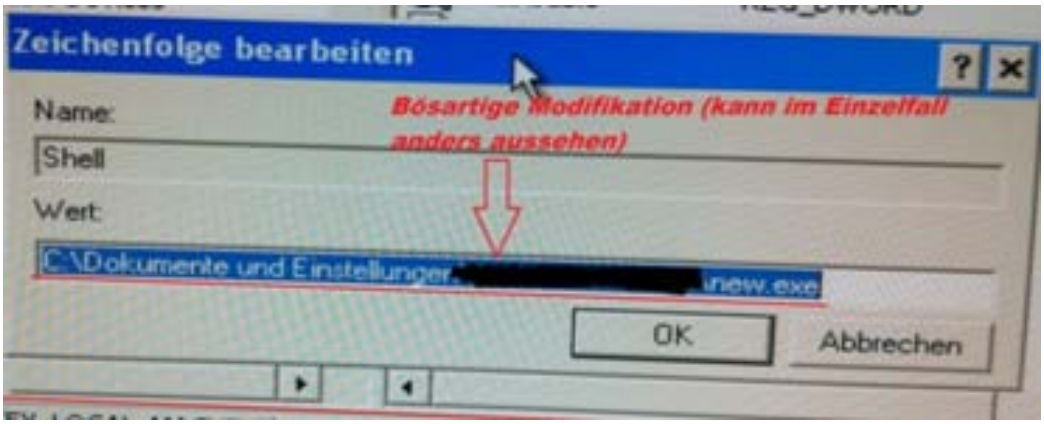
Phase 4

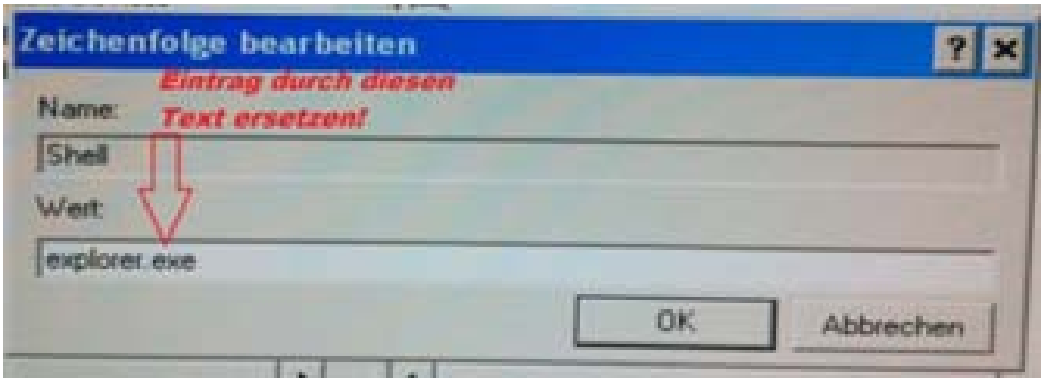
Un éditeur de la base de registre s'ouvre. Cherchez les entrées suivantes :

„HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon“

„HKEY_LOCAL_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon“

Pour retrouver les entrées, suivez l'arborescence de la base de registre. Cliqué sur « Winlogon » et sur la partie de droite de l'éditeur, vous verrez les clés à votre disposition. Cliquez deux fois sur la clé « Shell », une nouvelle fenêtre s'affiche: dans celle-ci, il y a la valeur « new.exe ». Veuillez changer cette valeur avec « **explorer.exe** ».





Phase 5

Redémarrez l'ordinateur à l'aide de l'ordre « shutdown –r ». L'ordre doit être donné dans la fenêtre de console. Attendez que les 30 seconds d'attente soient écoulées. Le système devrait redémarrer sans se bloquer.

Après le déblocage, nous conseillons de sauvegarder les données et de réinstaller le système.