

<http://softnology.biz/files.html>

Für die Installation Thaiphoon Burn muß man die Speicherintegrität als Administrator abstellen unter folgendem Pfad

A) Systemeinstellungen

- Einstellungen
- Datenschutz und Sicherheit
- Windows Sicherheit
- Gerätesicherheit
- Kernisolierung
- Details zur Kernisolierung

Option Speicherintegrität aus

Dann Neustart notwendig

B) Registry-Einstellungen von Win11 - Regedit ändern

- Terminal öffnen (geht einfach über windows suche „terminal“ eingeben)
- regedit.exe eintippen
- open the key
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CI\Config]
and set “VulnerableDriverBlocklistEnable”=dword:00000000

Dazu Vulnerable mit rechts anklicken- „ändern“
dann den Wert von 1 auf Null setzen und speichern (Einstellung hexa unverändert)

Dann Neustart notwendig

C) Nun kann man Thaiphoon nutzen

D) Uninstall und Rollback von Thaiphoon

Wenn man die Screenshots von Thaiphoon gespeichert hat, daran denken in den Systemeinstellungen die Speicherintegrität bei der Kernisolierung wieder zu aktivieren.

D.h. den kompletten Schritt A) wieder rückgängig

B) regedit rückgängig ist optional (d.h. Wert wieder auf 1 setzen. Geht aber schnell, weil regedit wieder im gleichen Pfad aufmacht.)

E) Treiber deinstallieren – ssgdio64.sys

Nachdem D) erledigt ist kommt beim nächsten Neustart die Fehlermeldung, dass der Treiber nicht geladen werden konnte: ssgdio64.sys

Dieser ist im Verzeichnis c:\Windows\SysWoW64\drivers
Diese Datei einfach manuell löschen. Dann ist es erledigt.