./ persistence-info.github.io

View on GitHub

AeDebug

Location:

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug`

Classification:

Criteria	Value
Permissions	Admin
Security context	User; System[1]
Persistence type	Registry
Code type	EXE
Launch type	Other
Impact	Non-destructive[2]
OS Version	All OS versions
Dependencies	OS only
Toolset	Scriptable

Description:

Well known key. Add or edit the `Debugger` value, using a REG_SZ string that specifies the command line for the debugger.

> If you want the debugger to be invoked without user interaction, add or edit the Auto value, using a REG_SZ string that specifies whether the system should display a dialog box to the user before the debugger is invoked. The string “1” disables the dialog box; the string “0” enables the dialog box.

Starts on application crash, which may be not reliable enough.

Breaks the parent-child chain, making it harder to detect.

References:

https://docs.microsoft.com/en-us/windows/win32/debug/configuring-automatic-debugging

Credits:

See also:

Remarks:

1. Depends on the crashing image ↩
2. The original debugger exe will not start ↩