./ persistence-info.github.io

View on GitHub

WER Debugger

Location:

`HKLM\Software\Microsoft\Windows\Windows Error Reporting\Hangs`

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:

> When applications hang, the Windows Error Reporting framework allows us to attach a debugger, if it is set up in the Registry. The actual key is present in this location:

```
HKLM\Software\Microsoft\Windows\Windows Error Reporting\Hangs\ Debugger
= <executable>
```

Relies on crashing applications, which may be not good enough for a real persistence. But it is Windows, something will crash sooner or later for sure.

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

References:

https://www.hexacorn.com/blog/2019/09/20/beyond-good-ol-run-key-part-116/

Credits:

@Hexacorn

See also:

Remarks:

1. Depends on the crashing process? ↩
2. The original debugger will not start ↩