.. /DumpMinitool.exe

Dump

Dump tool part Visual Studio 2022

Paths:
C:\Program Files\Microsoft Visual Studio\2022\Community\Common7\IDE\Extensions\TestPlatform\Extensions\DumpMinitool.exe

Resources:

- https://twitter.com/mrd0x/status/1511415432888131586

Acknowledgements:

- mr.d0x (@mrd0x)

Detections:

- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_dumpminitool_execution.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_dumpminitool_susp_execution.yml
- Sigma: https://github.com/SigmaHQ/sigma/blob/b02e3b698afbaae143ac4fb36236eb0b41122ed7/rules/windows/process_creation/proc_creation_win_devinit_lolbin_usage.yml

Dump

Creates a memory dump of the lsass process

```
DumpMinitool.exe --file c:\users\mr.d0x\dump.txt --processId 1132 --dumpType Full
```

Use case:	Create memory dump and parse it offline
Privileges required:	Administrator
Operating systems:	Windows 10, Windows 11
ATT&CK® technique:	T1003.001